經濟部

資訊服務業者落實個人資料保護暨資訊安全

參考指引

INDUSTRIAL DEVELOPMENT BUREAU, MINISTRY OF ECONOMIC AFFAIRS
經濟部工業局 編撰

中華民國110年12月

目錄

表目錄

圖目錄

第一章 前言

一、緣起

近年數位技術的發展，使各行各業開始投入數位經濟，其中資訊服務業因為所蒐集、處理或利用的個人資料數量龐大，種類也繁多，所產生之個資侵害風險明顯高於其他產業，例如網路購物、線上訂房等電子商務服務蓬勃發展，但隨之伴隨資訊安全事件（消費者、會員個人資料外洩等）時有所聞。電子商務、教育機構、社福機構等所架設的網站被駭的成因複雜，但通常不脫資安防護措施的疏漏所致，此時，受客戶委託建置網站前後台系統的資訊服務業者，更需要強化其資訊安全防護措施及個人資料保護安全維護措施。

因此，為了保護消費者的個人資料，做好資安防護及個人資料安全維護，成為現今從事數位經濟的企業組織所必須具備的營運條件。經濟部工業局為使資訊服務業者受電子商務等業者委託提供服務時，能提升個人資料保護管理能力及技術能力，促使業者能妥善保護及管理個人資料，並採取技術上及組織上相關的措施，來防止個人資料檔案被竊取、竄改、毀損、滅失或洩漏，特訂定《資訊服務業者落實個人資料保護暨資訊安全參考指引》供資訊服務業者參考。

二、指引內容與說明

（一）適用對象

本指引主要是供「提供資訊系統服務之資訊服務業者」（以下稱為「系統商」）參考，系統商受委託提供資訊系統服務之方式包含建置、維護、維運、代管等。例如開店平台系統、企業資源規劃 ERP 系統（Enterprise resource planning System）、飯店物業管理系統（Property Management System）等。

此外，其他「資訊服務業」，例如資訊軟體服務業（代碼 I301010）或電子資訊供應服務業（代碼 I301030），也都可參考本指引內容。

（二）重要觀念

需特別說明的是，系統商在遵循個資法相關規範時，除遵循最基礎的個人資料保護法外，尚須遵守所屬主管機關經濟部工業局所訂定「製造業及技術服務業個人資料檔案安全維護計畫管理辦法」。另外

依據個資法第 4 條規定，也需要遵守委託者主管機關訂定之相關法令規範。

（三）指引內容：PDCA

本指引採用「規劃—執行—檢查—改善」（Plan-Do-Check-Adjust，PDCA）過程模型，引導系統商建置個人資料保護暨資訊安全措施。本指引大綱如下：

第一章：說明編撰資訊服務業者受委託提供資訊系統服務之個人資料保護暨資訊安全參考指引緣起、本指引內容、重要觀念與提醒事項。

第二章：簡介個人資料保護暨資訊安全規劃（Plan），包含系統商可能的委託客戶業別，以及需考量的風險，包含營運風險（個資法令遵法成本、資安要求）及危害風險等。

第三章：簡介個人資料保護暨資訊安全實施（Do），就第二章提及之風險，說明事故發生前，平時可採取的維護措施的建構和實作，包含採取個人資料適當安全維護措施及資訊安全管理措施。

第四章：簡介個人資料保護暨資訊安全檢查（Check），就第三章的維護措施的建構和實作，進行是否落實的自我檢查或內部稽核，並搭配附錄的「自我檢查表」。

第五章：簡介個人資料保護暨資訊安全改善（Adjust），就第四章的檢查結果進行立刻矯正措施；以及當危害風險（個資事故）不幸發生時，系統商於事故發生中可採取的應對措施、事故發生後可採取的修補措施，以及需配合主管機關調查。

第六章：針對第三章及第五章的措施，介紹常見的問題案例。

附錄：提供「自我檢查表」，資服業者可用於檢視企業自身目前的個資暨資安準備情況，快速找出初步痛點並加以精進。另提供配合主管機關調查之佐證資料範例，協助業者於發生個資外洩事件需配合調查時，可盡快提供相關事證。

經濟部工業局希冀透過本指引，讓資訊服務業者受客戶委託提供服務時，能對於個人資料管理制度導入與遵循能有更多認知，並且在

《個人資料保護法》及相關法規要求的框架下，能以最低的成本和最高的效率完成個資保護措施。

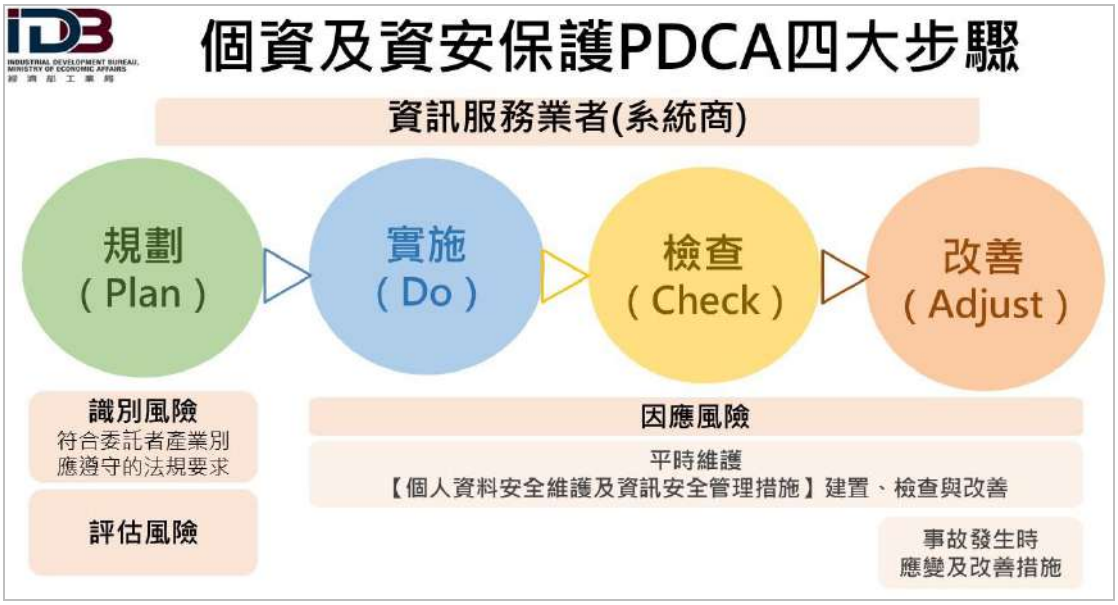

圖 1　個資及資安保護 PDCA 四大步驟

資料來源：本指引自製

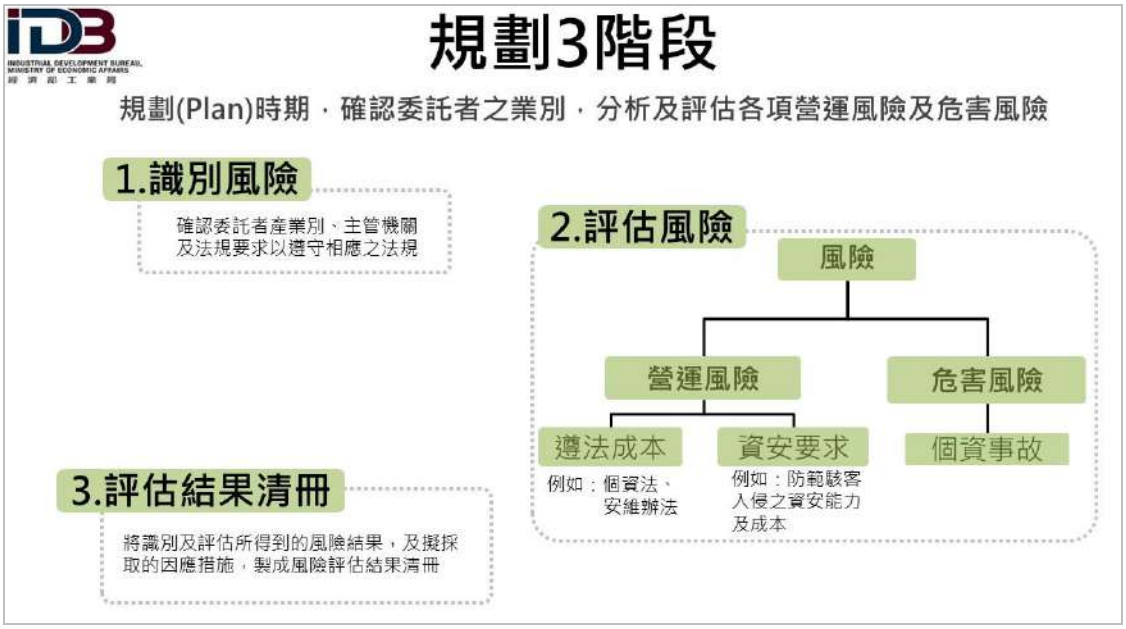

圖 2　規劃 3 階段

資料來源：本指引自製

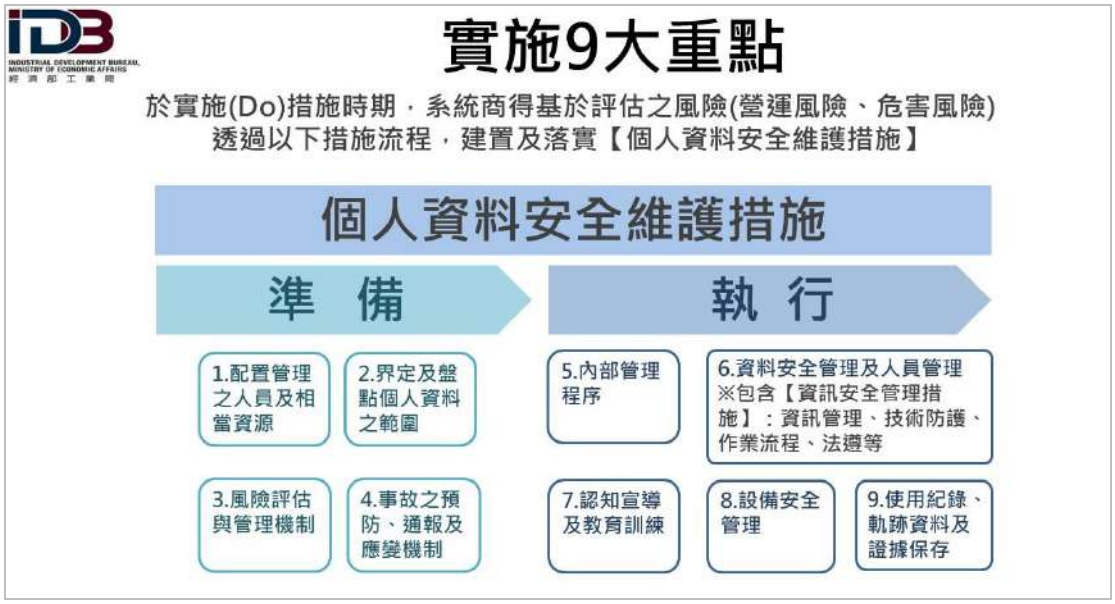

圖 3 實施 9 大重點

資料來源：本指引自製

圖 4 檢查 3 招式

資料來源：本指引自製

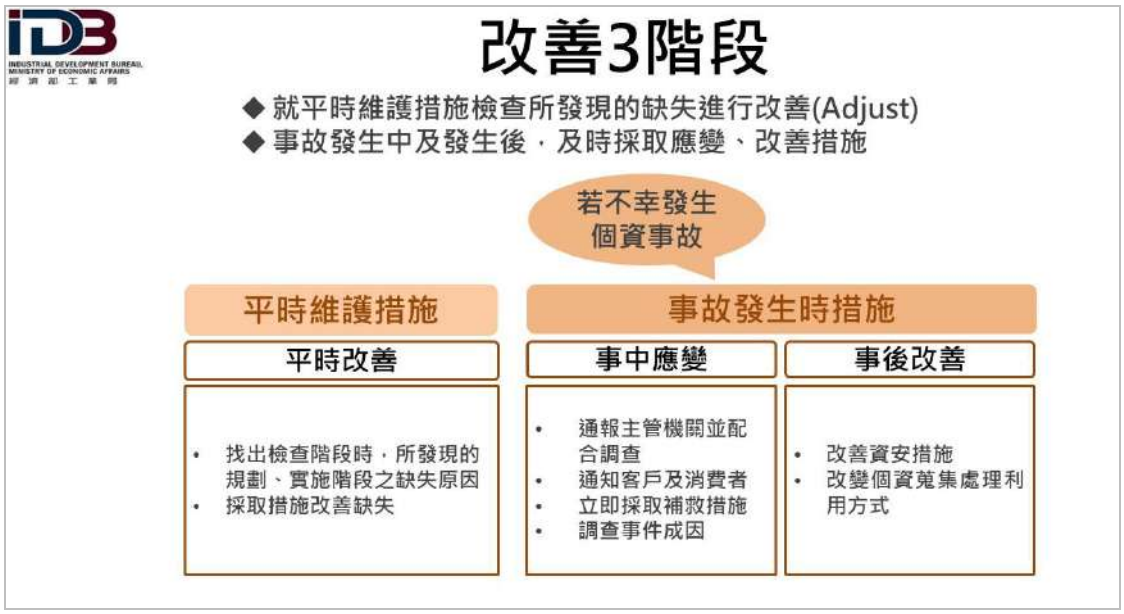

圖 5　改善 3 階段

資料來源：本指引自製

三、提醒事項

指引內所提示的義務，原則上做為系統商自我檢視之用。當發生資安事故而致個資侵害時，公司是否違反個人資料保護相關法令，仍宜依照具體事實認定之。

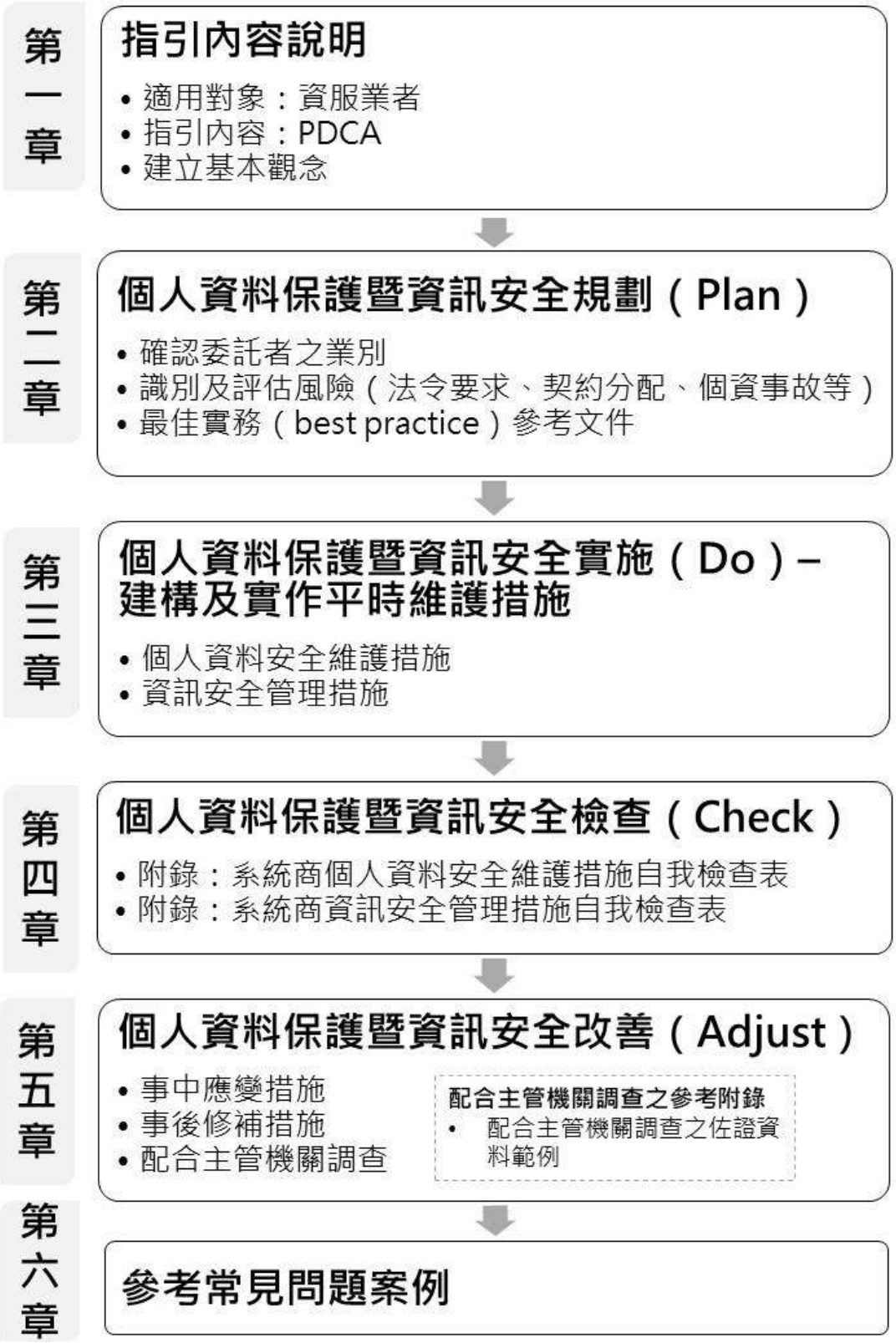

圖 6 指引內容大綱

資料來源：本指引自製

第二章 個人資料保護暨資訊安全規劃（PLAN）

系統商一開始應規劃建立個人資料保護暨資訊安全措施。可透過確認委託者之業別、分析與評估各項風險，風險包含須注意的營運風險（法令要求、資安要求）及危害風險（個資事故），以界定個人資料保護暨資訊安全措施之規劃範圍。

一、識別風險：確認委託者之業別

系統商受委託建置系統，依據個資法第 4 條規定：「受公務機關或非公務機關委託蒐集、處理或利用個人資料者，於本法適用範圍內，視同委託機關。」系統商受委託而於系統蒐集、處理、利用個人資料時，視同委託者之行為，因此系統商需要確認委託者的業別，並遵守委託者主管機關之相關法令規範及常見的最佳實務。

圖 7 個資法令及參考文件

資料來源：本指引自製

基於上述，以下將介紹系統商需注意及遵循之法令內容，並簡要說明常見的最佳實務，以協助業者能夠快速建立對於個資保護與資訊安全措施之基本觀念。

二、評估風險：受客戶委託提供資訊系統服務的風險

系統商在接受客戶委託提供資訊服務前，需考量與個人資料保護有關的措施並進行風險評估。綜觀目前企業採取個人資料保護有關之作為時，主要有營運風險（包含遵法成本與資安要求）及危害風險兩大項重點需做考量。

另外，可將識別及評估風險的結果，以及擬採取或已採取措施，製作風險評估結果清冊等文件化工作。

（一）營運風險：法令要求之遵法成本

個資相關法規範對於系統商的個資安全維護要求，系統商須納入事業經營的重要考量，若不加以重視，無法投入相應資金及人力等成本遵循相關要求，則可能產生個資事故之風險，例如個資不當蒐集、處理、利用，或者個資外洩。

系統商在遵循個資法相關規範時，應遵循最基礎的個人資料保護法、個人資料保護法施行細則、所屬主管機關經濟部工業局所訂定「製造業及技術服務業個人資料檔案安全維護計畫管理辦法」，以及依據個資法第 4 條規定遵守委託者主管機關訂定之相關法令規範。

1. 個人資料保護法及個人資料保護法施行細則

個人資料保護法的規範對象主要以「公務機關」與「非公務機關」兩大類來區分。

「非公務機關」係指公務機關以外的「自然人」、「法人」或其他團體（個資法第 2 條第 8 款），因此不論是個人、公司、民間團體都適用於個資法。此外，個資法並沒有設置適用門檻，亦即即使公司只保有 1 筆個資，一樣需要適用個資法相關規定。而所謂 1 筆，是指 1 個自然人的個資而言。

另外，個人資料保護法第 27 條規定，保有個人資料的企業組織，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。中央目的事業主管機關則可以指定非公務機關訂定個

人資料檔案安全維護計畫或業務終止後個人資料處理方法。

個人資料保護法施行細則就個人資料保護法的部分條文的細部作法，訂有較詳細的規定。例如就個人資料保護法第 27 條所稱「適當之安全措施」，施行細則於第 12 條規定 11 款措施事項。

2. 行政院資安處建議之資料安全管理措施

依據行政院於 110 年 8 月 11 日函頒之「行政院及所屬各機關落實個人資料保護聯繫作業要點」第 4 點規定，為強化資安標準規範，保有消費者交易、使用商品或接受服務等過程之一般或特種個資，且該資料達一定之適用門檻（如：個資數量、該業者資本額達一定金額或其他中央目的事業主管機關指定之特定標準）者，應依行政院資安處建議，至少訂定（一）使用者身分確認及保護機制、（二） 個人資料顯示之隱碼機制、（三）網際網路傳輸之安全加密機制、（四）個人資料檔案及資料庫之存取控制與保護監控措施、（五）防止外部網路入侵對策及（六）非法或異常使用行為之監控與因應機制等 6 項資料安全管理措施。詳細說明請見下表。

表 1 資料安全管理措施

管制措施	說明
一、使用者身分確認及保護機制	針對資通系統或個資檔案存取，提供使用者識別、鑑別及身分驗證管理機制，如帳密管制、多重認證技術、帳戶鎖定機制、密碼具一定複雜度等。(可參考資通安全責任等級分級辦法附表 10 相關作法)
二、個人資料顯示之隱碼機制	系統呈現介面上，如有個資資訊，應評估使用情境，予以適當且一致性之遮蔽，以為個資保護。
三、網際網路傳輸之安全加密機制	當個人資料進行網路傳輸時，應採用加密機制，包含使用加密傳輸管道、資料加密傳輸等。
四、個人資料檔案及資料庫之存取控制與保護監控措施	針對個人資料檔案及資料庫之儲存，應適當加密；存取時，應提供使用者識別、鑑別及身分驗證管理機制；留存相關日誌紀錄並定期檢視，或設置存取

	監控之系統化預警機制。
五、防止外部網路入侵對策	針對可能來自於網路的入侵，採取相關的偵測或防護作為，如個人電腦安裝防毒軟體、使用電子郵件過濾機制、設定網路防火牆、架構應用程式防火牆、採用入侵偵測及防禦機制或進階持續性威脅攻擊防禦措施等。
六、非法或異常使用行為之監控與因應機制	針對資通系統或個資檔案之存取，留存相關日誌紀錄並定期檢視，或設置存取監控之系統化預警機制。

資料來源：行政院資安處、行政院及所屬各機關落實個人資料保護聯繫作業要點

3. 製造業及技術服務業個人資料檔案安全維護計畫管理辦法

經濟部工業局為使所管行業能清楚了解個資法的主要內容，同時為加強製造業及技術服務業對於消費者個人資料之保護措施，故依個資法第 27 條第 3 項授權，訂定《製造業及技術服務業個人資料檔案安全維護管理辦法》（下稱安維辦法），具體規範了企業對於消費者個人資料保護及管理機制、告知義務、委託他人蒐集、處理或利用個人資料之監督、資料安全管理、消費者個人資料為國際傳輸前應遵循事項，以及改善機制等事項。

安維辦法第 2 條規定，保有 5000 筆以上消費者個人資料之製造業及技術服務業業者（以下簡稱業者），應依安維辦法規定，規劃、訂定、修正與執行消費者個人資料檔案安全維護計畫。因此，若系統商本身因直接蒐集（例如蒐集客戶承辦人個資）或間接蒐集（個人資料保護法第 9 條第 1 項，例如當事人同意電商將其個資委託系統商儲存），而保有 5000 筆以上的個人資料，則應遵守安維辦法之要求。不過，縱然業者所保有的消費者個人資料筆數未達 5000 筆而不適用安維辦法的規定，但仍須依照個人資料保護法辦理個資安全維護事項。

安維辦法第 6 條則規定了「72 小時通報義務」：「業者遇有消

費者個人資料安全事故，將危及其正常營運或大量當事人權益者，應於知悉事故後七十二小時內通報經濟部（以下簡稱本部），或通報直轄市、縣（市）政府時副知本部。.....」因此系統商遇有其所保有之個人資料被竊取、竄改、毀損、滅失或洩漏等個資安全事故時，應於知悉個資事故起 72 小時通報主管機關經濟部。

4. 常見的委託業別相關法規範

系統商依據個資法第 4 條規定，需要遵守委託者主管機關訂定之相關法令規範。而其委託者（以下亦稱客戶）之業別，可能為網際網路零售業、化粧品零售業（網路購物）；旅宿業者（線上訂房）；教育服務業、醫院、兒童課後照顧服務業、短期補習班業（會員管理系統）等。以下舉例系統商常見委託業別之主管機關訂定之「個人資料檔案安全維護計畫辦法」。

(1) 網際網路零售業及網際網路零售服務平台業

商業司有依個資法第 27 條第 3 項授權，訂定《網際網路零售業及網際網路零售服務平台業個人資料檔案安全維護計畫及業務終止後個人資料處理作業辦法》，該辦法第 2 條規定，以網際網路方式零售商品、登記資本額為新臺幣 1000 萬元以上、股份有限公司型態之網際網路零售業；或者以經營供他人零售商品之網際網路平台、登記資本額為新臺幣 1000 萬元以上、股份有限公司型態之網際網路零售服務平台業，應遵守該辦法之要求。因此受上述網際網路零售業及網際網路零售服務平台業委託之系統商亦應遵守該辦法。

而其餘的無店面零售業，包含郵購業（主計總處行業代碼 4871）、直銷業（主計總處行業代碼 4872）及未分類其他非店面零售業（主計總處行業代碼 4879），以及非新臺幣 1000 萬元以上股份有限公司型態之網際網路零售業及網際網路零售服務平台業，則暫不受該辦法之要求。

(2) 觀光旅館業

就觀光旅館業（營業項目代碼 J901011，主計總處行業代碼 5510），交通部有依個資法第 27 條第 3 項授權訂定《觀光旅館業個人資料檔案安全維護計畫辦法》。

(3) 其他教育服務業

就其他教育服務業（行業代碼 859），教育部亦有依個資法第 27 條第 3 項授權訂定《私立兒童課後照顧服務中心個人資料檔案安全維護計畫實施辦法》（兒童課後照顧服務業，營業項目代碼 JG01011，主計總處行業代碼 8595）、《短期補習班個人資料檔案安全維護計畫實施辦法》（短期補習班業，營業項目代碼 J201031，主計總處行業代碼 8595）等。

(4) 化妝品業及醫療器材業

衛生福利部依個資法第 27 條第 3 項授權預計訂有「醫療器材批發零售業個人資料檔案安全維護計畫實施辦法」草案（藥品及醫療用品批發業，主計總處行業代碼 4571；藥品及醫療用品零售業，主計總處行業代碼 4751）、「化粧品批發零售業個人資料檔案安全維護計畫實施辦法」草案（化粧品批發業，主計總處行業代碼 4572；化粧品零售業，主計總處行業代碼 4752）等。

(5) 高度監管行業

金融業、醫療業、電信業者等主管機關亦屬於高度監理機關，所訂定之個資相關法規範，如《金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法》、《醫院個人資料檔案安全維護計畫實施辦法》、《國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法》等，原則上也會較為嚴格，系統商受該些業別委託提供資訊系統服務時，應特別評估是否有能力遵循。

(6) 公務機關

系統商受政府委託建置和營運資訊系統，而被《資通安全管理法》指定為特定非公務機關時，系統商應同時注意資通安全管理法及相關規範。例如「資通安全事件通報及應變辦法」規定，知悉資通安全事件後，應於 1 小時內依中央目的事業主管機關指定之方式，進行資通安全事件之通報，並於 36 小時（第 3、4 級資通安全事件）或 72 小時（第 1、2 級資通安全事件）內完成損害控制或復原作業並通知處理事宜，往後 1 個月內持續進行事件之調查及處理，並送交調查、處理及改善報告。

（二）營運風險：契約與責任分配之遵法成本

系統商與委託者所訂定的契約，有關個人資料安全維護措施部分，可以在不違反個資法的情況下，訂定雙方的權利及責任分配。

換言之雙方應於締結契約時，即對於系統商和客戶間的個資安全維護要求，釐清權責分配。而系統商一旦締約，同樣應將締約內容納入事業經營的重要考量，包含投入資金及人力等成本遵循相關要求，以免產生個資事故之風險時，發現實際上無力遵循。

（三）營運風險：資安要求

近年發生的個資外洩，通常涉及資訊安全問題，為了保護消費者的個人資料，做好資安防護，成為現今從事數位經濟的企業組織所必須具備的營運條件。因此系統商受委託建置資訊系統服務時，系統商自身必須評估，其所掌握的資安能力、水準及資金成本，是否足夠防範駭客入侵所產生的個資外洩或其他個資事故。

若是因為系統商本身的系統漏洞，造成個資外洩等事故發生，則可能被認定為未為適當的個人資料安全維護措施，仍可能違反個資法第 27 條規定，而被主管機關依同法第 48 條裁罰。

（四）危害風險：個資事故

近年的個資事故型態，不同於早期的不當蒐集、處理、利用個資之情形，現在更多是個資外洩（即洩漏及竊取）事件。系統商受客戶委託提供資訊服務所使用的資訊系統，也逐漸成為駭客攻擊的主要對象。當資訊服務網頁或資訊系統本身有系統漏洞，或系統商企業內部未防範資安事故，都有可能造成個資外洩事故。

因此平時評估前台網頁、後台系統、公司內部之個資及資安風險類型及對策，成為防範個資外洩事故風險重要的課題[1]。或在不幸發生個資事故時，迅速且妥善的在事發時應變，以及事發後修補，都能減少損害和損失。

---

[1] 評估風險類型及對策的參考表及評估清冊等文件化內容，可參經濟部工業局，〈資訊服務業提供服務之個資保護及案例說明手冊〉，經濟部工業局 106 年製造業價值鏈資訊應用計畫，頁 31，https://www.moeaidb.gov.tw/22external/ctlr?PRO=filepath.DownloadFile&f=news&t=f&id=7818（最後瀏覽日：2021/12/20）。

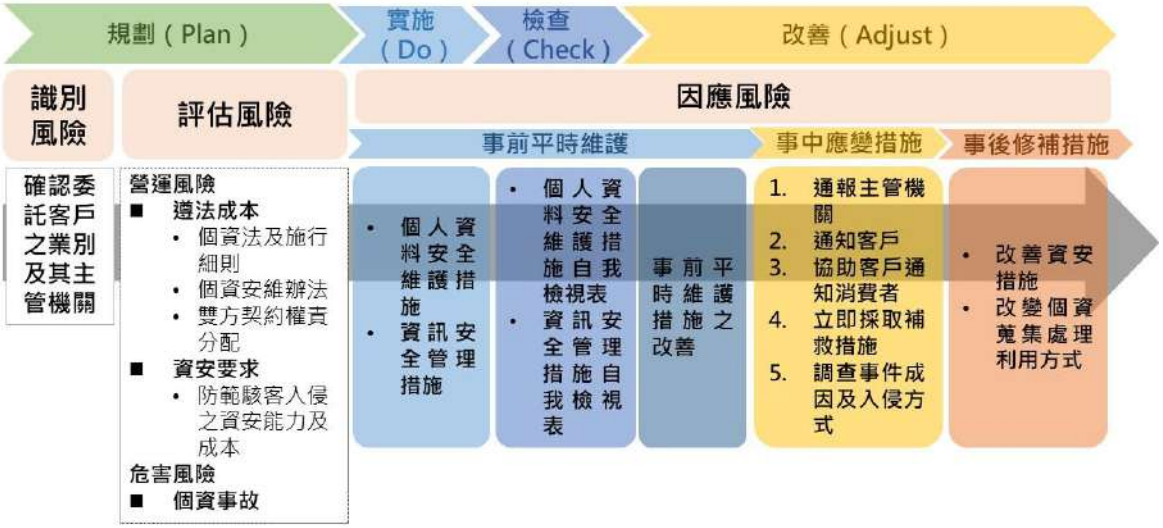

圖 8 系統商提供資訊系統服務之風險評估及管理流程圖
資料來源：本指引自製

三、最佳實務（best practice）參考文件

系統商除應遵循之法規範外，亦可參考以下個人資訊管理系統與資訊安全管理系統國際標準，以及其他產業主管機關所發布的指引，據以建立企業內部完整的管理制度，以更完整的強化整體個資及資安管理體系。

（一）資訊安全管理系統與個人資訊管理系統國際標準

ISO/IEC 27001 資訊安全管理系統（Information Security Management System）是目前國際上最多企業組織遵循的資訊安全管理系統，企業組織可透過 ISO/IEC 2700 建置符合需求的資訊安全控制措施，以達成一定水準的資安防護能力。[2]

ISO/IEC 27701 個人資訊管理系統（Privacy Information Management System）是建立在 ISO/IEC 27001 之上，在資訊安全擴充及強化個人資料隱私要求和控制措施的管理系統，並整合 ISO 27001、ISO27002、ISO 29100 等實務做法。[3]

（二）其他業別主管機關參考指引

[2] ISO/IEC 27701 隱私資訊管理 個人資訊保護的當責與信任，BSI，https://www.bsigroup.com/zh-TW/iso-27701/（最後瀏覽日：2021/12/20）。
[3] ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines, ISO, https://www.iso.org/standard/71670.html (last visited Dec. 20, 2021).

系統商受客戶委託提供系統服務，依據個資法第 4 條規定，系統商受委託而於系統蒐集、處理、利用個人資料時，視同委託者客戶之行為，因此建議系統商也應參考與遵循委託者客戶所屬產業主管機關訂定之最佳實務參考文件。

目前主要有經濟部商業司針對無店面零售業之電子商務交易及資訊安全訂定相關指引與參考文件。包含 101 年訂定「電子商務交易安全規範(網路平台、供應商、物流商)修正版」[4]、104 年訂定「電子商務個資外洩資安防護參考指引」[5]、106 年訂定「小型電子商務業者資安與個資防護參考指引」[6]（內含「網路零售業資安基本查核表說明」）等參考指引，系統商可於遵循本指引之餘，亦視委託客戶之屬性參考上述指引。

（三）TWCERT/CC

「台灣電腦網路危機處理暨協調中心（TWCERT/CC）」在行政院資通安全處及國家通訊傳播委員會指導下，協處企業資安事件通報、通報產品資安漏洞、惡意檔案檢測服務，並蒐集及共享國內外 CERT/CSIRT、資安組織、學研機構、民間社群、政府單位及私人企業間的資安情資，以及舉辦資安推廣宣導活動等，其提供之資訊對於提升我國業者資安聯防能量及網路安全極有參考價值。

因此，鼓勵系統商至「台灣電腦網路危機處理暨協調中心（TWCERT/CC）」網站首頁[7]，申請加入「台灣 CERT/CSIRT 聯盟」會員，便於接收國內資安事件情資分享，強化資安自我防禦能量。

---

[4] 財團法人資訊工業策進會編製，〈電子商務交易安全規範(網路平台、供應商、物流商)修正版〉，經濟部商業司 101 年度電子商務交易安全及資安服務平台推動計畫，101 年 11 月，https://www.cnra.org.tw/edm/ec-cert_1.pdf（最後瀏覽日：2021/12/20）。

[5] 財團法人資訊工業策進會編製，〈電子商務個資外洩資安防護參考指引〉，經濟部商業司 104 年度電子商務交易安全推動計畫，104 年 7 月，https://www.cnra.org.tw/edm/ec-cert_2.pdf（最後瀏覽日：2021/12/20）。

[6] 財團法人資訊工業策進會編製，〈小型電子商務業者資安與個資防護參考指引〉，經濟部商業司 104 年度電子商務兆元推動計畫，105 年 8 月，https://www.cnra.org.tw/index.php?action=download&cid=160&id=381（最後瀏覽日：2021/12/20）。

[7] 台灣電腦網路危機處理暨協調中心（TWCERT/CC），https://www.twcert.org.tw/tw/mp-1.html（最後瀏覽日：2021/12/20）。

第三章 個人資料保護暨資訊安全實施（DO）：建構及實作平時維護措施計畫

為因應個資事故之危害風險、個資法遵成本及資安要求等營運風險，企業組織應於事故發生前（事前）做好維護措施、事故發生時（事中）採取應變措施、事故發生後（事後）採取修補措施。

本章主要說明事前之平時維護措施之實施部分（參下圖 4）。

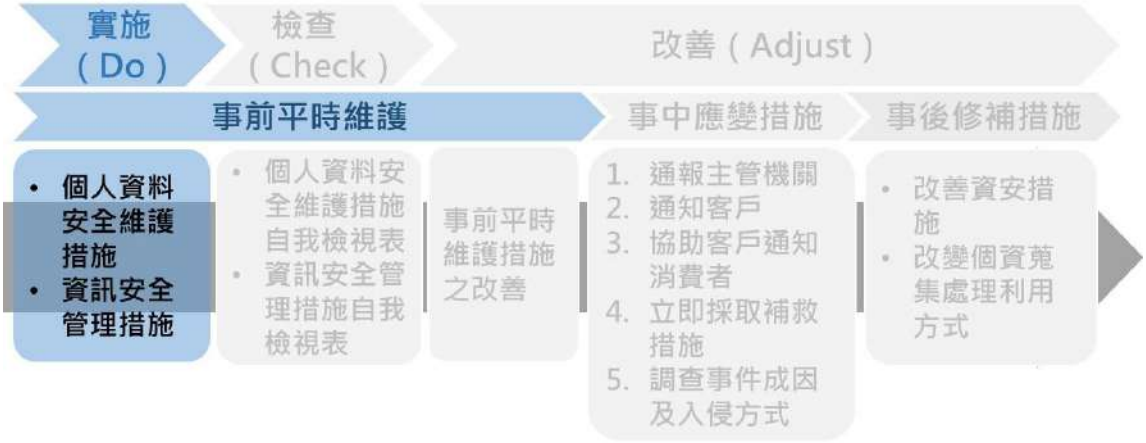

圖 9 因應風險應採取之措施流程圖－事前實施
資料來源：本指引自製

為因應上述風險，系統商首先應依據前述規劃所界定的適用範圍及識別的風險，建構及實作一套風險處理計畫，亦即「個人資料保護暨資訊安全平時維護措施計畫」之實施。換言之，企業組織應採行適當安全措施，防止個資被竊取、竄改、毀損、滅失或洩漏（參個資法第 27 條第 1 項規定）。所謂「適當安全措施」，包括：

1. 個人資料安全維護措施：針對個人資料檔案安全維護，採取「組織管理」上之措施，擬訂內部管理作法。

2. 資訊安全管理措施：就個人資料檔案安全維護中的「資料安全管理」，採取「資安技術」上之管理措施，訂定並落實「資訊安全管理政策」。「資訊安全管理措施」其實屬於「個人資料安全維護措施」中的一部分，惟近年個資外洩事件多與資安防護作為有關，因此資訊安全管理措施也被視為適當安全措施中重要的一個環節。

完整的「個人資料保護暨資訊安全平時維護措施計畫」，包含「準備」、「執行」、「檢查」、「改善」四個階段。「準備」及「執行」，屬於個資保護及資訊安全 PDCA 四大步驟中的「實施」（Do）步驟。

因此，本文將「個人資料保護暨資訊安全平時維護措施計畫」之實施，分為「準備」、「執行」兩個階段，並先介紹「個人資料安全維護措施」，再說明其中的「資訊安全管理措施」。

至於資料安全稽核機制（包含自我檢查、內部稽核、外部稽核等）「檢查」（Check）步驟，於本指引第四章說明。個人資料安全維護及資訊安全管理的整體「改善」（Adjust）步驟，於本指引第五章說明。

但為完整呈現個人資料安全維護措施及資訊安全管理措施流程，下圖將準備、執行、檢查、持續改善等流程完整呈現。

圖 10 建置個人資料適當安全維護措施流程

資料來源：本指引自製

一、個人資料安全維護措施

本指引參考個人資料保護法、個人資料法護法施行細則第 12 條[8]、經濟部「製造業及技術服務業個人資料檔案安全維護管理辦法」及國際標準 ISO 27001 資訊安全管理系統、ISO27701 個人資訊管理系統等內容，提出「個人資料檔案安全維護措施」建議，並包含資訊服務提供者之特有個資保護議題。

針對「個人資料檔案安全維護措施」建議作法，以下將依序說明 11 項措施（參考圖 6）。此外，企業組織並應將此些措施撰擬作成「個人資料安全維護計畫」[9]文件。

（一）配置管理之人員及相當資源

1. 個資保護總負責人

公司應有高階管理階層成員擔任個資保護總負責人[10]，其應具統籌各部門之能力，並能提供資源、協調與推動個資保護相關事宜，以利個人資料安全維護事項之運行。並必須檢驗所有資料保護的防護措施部署的執行，並檢驗其是否正確完成。

2. 個資管理專員

---

[8] 個人資料法護法施行細則第 12 條：「本法…第二十七條第一項所稱適當之安全措施，指公務機關或非公務機關為防止個人資料被竊取、竄改、毀損、滅失或洩漏，採取技術上及組織上之措施。
前項措施，得包括下列事項，並以與所欲達成之個人資料保護目的間，具有適當比例為原則：
一、配置管理之人員及相當資源。
二、界定個人資料之範圍。
三、個人資料之風險評估及管理機制。
四、事故之預防、通報及應變機制。
五、個人資料蒐集、處理及利用之內部管理程序。
六、資料安全管理及人員管理。
七、認知宣導及教育訓練。
八、設備安全管理。
九、資料安全稽核機制。
十、使用紀錄、軌跡資料及證據保存。
十一、個人資料安全維護之整體持續改善。」

[9] 製造業及技術服務業個人資料檔案安全維護管理辦法第 2 條第 1 項：「保有消費者個人資料之製造業及技術服務業業者，應依本辦法規定，規劃、訂定、修正與執行消費者個人資料檔案安全維護計畫。」

[10] 所謂由高階管理階層擔任個資保護總負責人，係指由總經理、代表人擔任，或至少副總經理級、法遵長、總稽核，小規模企業由法務長擔任亦可。

公司應配置管理人員（一位或以上）辦理個人資料保護法第27 條所稱之安全維護事項之落實。若組織較為龐大，各部門可皆安排一位個資管理人員。

公司的總管理專員建議以專責為宜，專責的好處在於，除了能最熟悉公司之個資事務外，亦可接受各種外訓，例如 ISO 27001、ISO27701 等國際標準，並進而能成為合格的公司內稽人員。

（二）界定及盤點個人資料之範圍

1. 蒐集處理利用個人資料之告知

公司要蒐集、處理、利用個人資料時，應對當事人說明個人資料的蒐集、處理及利用之特定目的及特定情形（參見個人資料保護法第 19 條第 1 項各款），以及說明個人資料類別、利用期間、利用地區及利用方式等。之後應將說明內容，寫入個人資料檔案安全維護計畫。

2. 界定個人資料之範圍

公司可能就員工、客戶承辦人、上下游供應商承辦人等的個資，蒐集處理利用。另外，系統商提供資訊服務時，雖然非未主動蒐集，但受委託傳輸、儲存個資，而有處理個資；或者雖未儲存個資，但建置於客戶端的資訊系統發生故障，系統商維修時可能接觸儲存在資訊系統內的個資。

個人資料之範圍，包含個人資料保護法第 2 條例示的項目（自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動），以及其他得以直接或間接識別個人的資料，例如生理資訊、車輛維修紀錄、行車紀錄等。

建議使用法務部訂定之「個人資料保護法之特定目的及個人資料之類別」[11]（包括代號）敘明所蒐集個資之特定目的及類別，例如：「特定目的〇〇一人身保險」;「個人資料類別 C0 一一個人描

[11] 個人資料保護法之特定目的及個人資料之類別，法務部主管法規查詢系統，https://mojlaw.moj.gov.tw/LawContent.aspx?LSID=FL010631（最後瀏覽日：2021/12/20）。

述。例如：年齡、性別、出生年月日、出生地、國籍、聲音等」。

3. 個人資料盤點

蒐集個人資料後，應進行盤點，應計算及呈現個人資料筆數。盤點做法沒有特定，雖沒有絕對精準無疏漏的盤點方式，但建議可使用「分析個資流程」方式，盤點出公司所蒐集、處理、利用之個人資料。分析個資流程內容包括下列項目：[12]

(1) 清查各作業流程中所使用之表單、紀錄，並辨識個人資料有關之表單、紀錄，歸納整理成個人資料檔案。

(2) 使用個人資料盤點表檢視其保有之個人資料檔案，確認個人資料檔案名稱、保有之依據及特定目的、個人資料種類。

(3) 使用個人資料盤點表檢視其保有之個人資料檔案之生命週期及其適法性，包含蒐集、處理、利用之過程及是否合法。

（三）風險評估與管理機制

透過上述所界定和盤點之個人資料，建立個人資料風險評估及管理機制，風險評估係識別導致風險之原因，風險管理則在於研擬風險對策。

1. 風險評估

(1) 系統或設備之風險評估

公司應針對內部電腦及內外部資訊系統，以及儲存電商客戶或旅宿業客戶之消費者個人資料之系統或設備進行盤點，為個人資料可能被竊取、竄改、毀損、滅失或洩漏之風險評估。

(2) 蒐集、處理、利用作業之風險評估

公司應針對個人資料之蒐集、處理與利用時，產生的各種作業情境及內容，進行個人資料可能被竊取、竄改、毀損、滅失或洩漏之風險評估。

---

[12] 另可參經濟部工業局，〈資訊服務業提供服務之個資保護及案例說明手冊〉，經濟部工業局 106 年製造業價值鏈資訊應用計畫，頁 21 以下，https://www.moeaidb.gov.tw/22external/ctlr?PRO=filepath.DownloadFile&f=news&t=f&id=7818（最後瀏覽日：2021/12/20）。

作業情境及內容，可能包含加工（例如輸入、編輯、輸出、掃描等）、傳輸（內外部傳輸，可能透過 E-mail、網路伺服器等傳輸）、保管儲存（載體包含個人電腦、資料庫、主機伺服器；風險態樣例如不當存取、個人電腦遭外部攻擊等）、廢棄（例如刪除、資料銷毀不夠落實致外洩）。

2. 風險管理

針對前述風險評估之結果，提出預定或已採取之具體風險管理措施或風險處理對策，並將評估結果結合擬採取或已採取措施及個資盤點表，進行文件化工作，例如製作「個人資料風險評估清冊」。

（四）事故之預防、通報及應變機制

1. 事故預防

公司應制定事故之預防、通報(當事人及主管機關)及應變機制，並建議以流程圖呈現。

每年應至少進行一次事故演練並進行相關檢討。

2. 事故通報

(1) 通報主管機關

依《製造業及技術服務業個人資料檔案安全維護管理辦法》第 6 條規定：

A. 通報時點：知悉發生事故 72 小時內。

B. 通報條件：業者遇有消費者個人資料安全事故，將危及其正常營運或大量當事人權益者。

C. 通報對象：業者應通報經濟部，或通報地方政府時副知經濟部。

D. 通報內容：事件發生種類、外洩大略筆數、發生原因及事件摘要、採取的因應措施、通知當事人的時間和方法。

(2) 通知客戶業者及其消費者

通知當事人部分，理論上應由與消費者直接接觸、蒐集消費者個資之業者（例如電商業者、私人醫院診所、私立學校、非營利組織等），依個人資料保護法為通知。

不過系統商與其客戶基於契約關係，協助客戶代管主機或儲存資料時，因而保有消費者個資，因此當知悉消費者個資因資安事故有外洩等情形時，應立即通知客戶業者，並可基於與客戶的契約關係，協助客戶業者以下事宜：

A. 可受客戶業者委託，協助代為通知消費者。但通知內容是否合於個資法規定，最終仍應由客戶業者自行負責。

B. 提醒客戶業者通報其主管機關。

C. 提供發現事件時立即調查的情形，供客戶業者通報主管機關及通知消費者。

以下為《個人資料保護法》第 12 條[13]、《個人資料保護法施行細則》第 22 條[14]所規範的適當通知方式：

A. 通知時點：自知悉時起即應盡速通報。

B. 通知條件：業者遇有消費者個資被竊取、洩漏（個資外洩）或竄改、損毀、滅失之事故。

C. 通知內容：使消費者知悉個資遭外洩或竊取、已採取哪些因應對及修補措施。而非僅是防詐騙宣導。

D. 通知方式：以簡訊、電子郵件等其他足以使當事人知悉或可得知悉之方式。

3. 事中應變及事後修補改善措施

---

[13] 《個人資料保護法》第 12 條：「公務機關或非公務機關違反本法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人。」

[14] 《個人資料保護法施行細則》第 22 條：「本法第十二條所稱適當方式通知，指即時以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之。但需費過鉅者，得斟酌技術之可行性及當事人隱私之保護，以網際網路、新聞媒體或其他適當公開方式為之。（第 1 項）依本法第十二條規定通知當事人，其內容應包括個人資料被侵害之事實及已採取之因應措施。（第 2 項）」

公司應於事故時採取必要措施（應變機制），以及事故發生後採取修補改善措施。

事故發生時所採取之應變措施，包含列舉發生時、發生後之可能做法或執行流程，例如：

(1) 立即通報主管機關

(2) 立即通知客戶

(3) 協助客戶通知其消費者

(4) 立即採取補救措施（尋找惡意程式等）：可透過惡意程式偵測或數位鑑識等方式。若損害層面過大，建議必要時可考慮先將涉及外洩客戶部分之系統伺服器暫停營運（停機）。另外，應採取最基礎的停止損害措施，例如立刻限制國外 IP 存取、限縮客戶帳號存取權限等。

(5) 調查事件成因及入侵方式（包含本身系統及網站，以及協助客戶）：調查事件成因之方式，包含調取 log 查閱是否有異常 IP、透過資安健檢尋找後台系統及前台網站漏洞（包含原碼檢測、滲透測試、弱點掃描等）、研究駭客路徑找出其他可能成因（例如員工遭受社交工程攻擊並上當）等。

事故發生後則進行改善修補措施之方式，降低、控制當事人損害，例如：

(1) 改善資安措施：透過已釐清之事件成因進行弱點漏洞修補、部分或全面改善系統資安防護措施等（例如系統架構變更、強化防火牆、傳輸渠道加密、資料庫加密等）。

(2) 改變個資蒐集處理利用方式：包含採取個資最小化措施（例如傳輸個資時遮罩隱碼）、改變個資蒐集內容、改變個資傳輸方式、改變個資儲存地點及方式等。

(3) 重新評估與客戶間資安責任：評估客戶是否能承擔改善修補後的資安保護能力成本，重新以契約約定雙方資安責任，或者於客戶無力負擔時不再與該客戶續約，以免使系統商本身承受過多危害風險。

（五）內部管理程序

為確保個人資料之蒐集、處理或利用符合個人資料保護法規定，應採取個資的內部管理程序。

1. 個人資料之蒐集、處理或利用程序

(1) 蒐集

包含蒐集方式(以何種方式蒐集之個人資料)、目的告知(如何向當事人告知蒐集之目的，或變更使用之目的)、檢視目的(如何檢視蒐集是否符合個資保護相關法令要求的特定目的)。

(2) 處理

以何種方式記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結及內部傳送個資；如何檢視處理個資時是否符合個資保護相關法令要求的特定目的。

(3) 利用

以何種方式利用及行銷、資料；當事人若拒絕行銷時的後續處理機制為何。

(4) 特定目的已消失或期限已屆滿

定期檢視消費者個人資料蒐集之特定目的是否已消失或期限是否已屆滿；其特定目的消失或期限屆滿者，並應確保符合個資法第 11 條第 3 項之規定。

2. 受理當事人行使權利之程序

(1) 告知義務

除有免告知事由，公司應對資料當事人踐行告知「當事人得行使權利」之義務：

A. 告知當事人得依個資法第 3 條規定得行使之權利及方式，包含查詢或請求閱覽、請求製給複製本、請求補充或更正、請求停止蒐集、處理或利用、請求刪除等。

B. 告知當事人得自由選擇提供個人資料時不提供將對其

權益之影響。

(2) 受理程序

公司應採取措施，確保能完整進行受理當事人行使權利之程序，包含規劃程序並在個人資料安全維護計畫中敘明。以免未確實依照當事人要求處理個資，而不當處理及利用個資，例如當事人已要求刪除個資，但公司未實際刪除，持續利用該當事人個資進行行銷或其他利用。

公司並應向個資當事人知悉公司受理當事人行使權利之程序，使當事人知悉的方式，除文字外，建議提供受理流程圖。

3. 國際／境外傳輸

(1) 檢視是否受主管機關限制

公司若將消費者個人資料作國際傳輸者，應檢視是否受主管機關經濟部限制。公司將資料傳輸到位在我國以外國家地區之伺服器或資料庫，則有個人資料為國際／境外傳輸之情形。

(2) 告知「個資有國際／境外傳輸」義務

有國際／境外傳輸情形者，公司應踐行告知資料當事人，其個人資料會傳輸至我國以外地區，並進行處理、利用，使我國的資料當事人得以知悉個人資料之利用地區將不限於我國境內。

4. 委託他人蒐集、處理或利用個人資料之管理程序

如果公司有委託他人蒐集、處理、利用個人資料之情形，公司應對受託者進行個資安全維護之監督管理（個人資料保護法施行細則第 12 條）。例如公司與受託者於契約中敘明個資安全維護責任之事項、對受託者進行稽核 1 年至少 1 次等。

5. 業務終止後有關於個人資料之處理方式

(1) 特定業務減少或終止

公司應訂定有關業務如有減少或其特定業務項目被終止，個人資料處理方法。例如個資刪除之程序及佐證，或個資移轉之原因、對象、方法、時間、地點，以及受移轉對象得保有該個人資

料之合法依據。

並踐行個人資料保護法第 9 條所定之告知義務，以使資料當事人知悉其個人資料被移轉至他公司。若當事人不同意移轉，應使當事人能行使個資法第 3 條之權利。

(2) 法人格消滅

公司應訂定有關法人格被消滅時個人資料處理方法。例如法人格消滅後如有將個人資料移轉予其他法人之情形，應記錄其原因、對象、方法、時間、地點，以及受移轉對象得保有該個人資料之合法依據。

並踐行個人資料保護法第 9 條所定之告知義務，以使資料當事人知悉其個人資料被移轉至他公司。若當事人不同意移轉，應使當事人能行使個資法第 3 條之權利。

（六）資料安全管理及人員管理

1. 資料安全管理措施

主要內容請見本指引之【資訊安全管理措施】。下述為法規要求。

公司應就資料存取控制、保存、傳輸等，採取管理措施，包括但不限於資料之加密機制、對備份資料採取適當保護措施、傳輸資料時採取適當保護措施、使用者認證機制、異常存取監控機制等。（製造業及技術服務業個人資料檔案安全維護管理辦法第 8 條第 1 項）

公司以資訊系統處理個資時，應採取適當管理措施，包含：（製造業及技術服務業個人資料檔案安全維護管理辦法第 8 條第 2 項）

(1) 防火牆：建置防火牆或其他入侵偵測設備。

(2) 防毒軟體：與網際網路相聯之資訊系統存有消費者個人資料者，應安裝防毒軟體，定期更新病毒碼，並執行掃毒作業。

(3) 弱點掃瞄及修補：針對電腦作業系統及應用程式之漏洞，定期安裝修補程式。

(4) 密碼及認證機制：資訊系統存有消費者個人資料者，應設定認證機制，其帳號及密碼須符合一定之複雜度。

(5) 異常存取行為監控：資訊系統存有消費者個人資料者，應設定異常存取資料行為之監控機制。

(6) 避免利用真實個資測試：處理消費者個人資料之資訊系統進行測試時，應避免使用消費者真實個人資料；使用消費者真實個人資料者，應訂定使用規範。

(7) 資訊系統變更：處理消費者個人資料之資訊系統有變更時，應確保其安全性未降低。

(8) 定期檢查：定期檢視處理消費者個人資料之資訊系統，檢查其使用狀況及存取個人資料之情形。

(9) 個資隱碼：透過 API 傳輸個人資料時，以及提供電子商務服務時，應評估採行消費者個人資料之隱碼機制，就個人資料之呈現予以適當且一致性之遮蔽。（系統商進階建議）

2. 人員安全管理措施

公司應採取人員保密義務約定、人員進出管制措施、人員保密措施、人員存取權限之控制、人員離退時之資料返還等管理措施。（製造業及技術服務業個人資料檔案安全維護管理辦法第 10 條）

公司若採取分散式管理，或沒有固定辦公場所，仍應為人員存取、資料返還等管理措施執行之紀錄。

（七）認知宣導及教育訓練

公司應對內部員工及外部客戶，採取認知宣導或教育訓練措施。

1. 內部員工教育訓練

公司應對其所屬員工進行個人資料保護教育訓練，並加強要求員工接受訓練。教育訓練應至少包含以下規劃：（1）訓練內容：個人資料保護相關法令之規定；所屬人員之責任範圍；本計畫各項管理程序、機制及措施之要求（製造業及技術服務業個人資料檔案安全維護管理辦法第 11 條）；（2）頻率：敘明實施頻率，並至少於公司資安或個資政策更新時實施；（3）程序：訂定實施頻率，每次宣

導或訓練時訂定主題、議程，且實施簽到、製作會議紀錄、課後評量機制。

2. 外部客戶認知宣導

公司宜對其客戶進行個人資料保護認知宣導，包括但不限於在契約簽訂前，向該客戶揭露雙方之個人資料安全維護措施。

公司於認知宣導時，宜建議客戶使用系統時應備有安全環境，例如登入系統之電腦應加裝防毒軟體並定期掃毒、上傳資料至系統前應先進行惡意程式偵測、應定期進行防範社交工程訓練、不上有資安風險之網站等。

（八）設備安全管理措施

公司應對於存有個人資料之紙本、光碟片、電腦、自動化機器設備及其他媒介物等，採取設備維護安全管理措施及儲放環境安全管理措施。包含人員管理規範、人員進出管制、防水防震防火等適當之保護設備或技術。（製造業及技術服務業個人資料檔案安全維護管理辦法第 12 條）。

公司對於過期資料及軟硬體的處理方式應採取措施。例如提供新版本之資料及軟硬體時，應繳回或刪除舊版本。

（九）使用紀錄、軌跡資料及證據保存

1. 使用紀錄及軌跡資料證據保存

執行個人資料檔案安全維護計畫時，保存下列紀錄至少五年：（1）個人資料使用紀錄；（2）自動化機器設備之軌跡資料；（3）落實執行個人資料檔案安全維護計畫之證據。

2. 因業務終止而銷毀證據保存

因業務終止而銷毀個人資料者，記錄其方法、時間及地點；移轉個人資料者，記錄其原因、對象、方法、時間、地點及受移轉對象得保有該個人資料之合法依據。其他刪除、停止處理或利用個人資料者，記錄其刪除、停止處理或利用之方法、時間或地點。

二、資訊安全管理措施

企業組織應於平時，就個人資料管理措施之「資料安全維護措施」，實施「資訊安全管理措施」，強化資安保護措施，以預防資安事故（例如個資外洩）的發生。

平時的資安管理措施，可以從營運管理面、技術防護面、作業流程面、維護、遵循性及持續改善等面向，多方面齊下以防護資安。本指引參考國際標準 ISO/IEC 27001 資訊安全管理系統之內容，提出資訊安全管理措施之執行及政策訂定的建議，並特別包含提供資訊系統服務之特有資安議題。

（一）營運管理面

1. 資訊安全權責

(1) 由高階管理者擔任資訊安全總負責人：資訊安全總負責人可由總經理、代表人擔任、副總經理級或資安長級擔任，即能統籌各部門、協調與推動資安防護相關事宜及所需之資源，且須檢驗所有資訊保護的防護措施的正確完成執行者即可。

(2) 資訊安全總負責人應確保有關資安角色與職權之分配與傳達：明訂與分配組織內部所有資訊安全責任，並確實賦予權利執行。另外，也應注意將相互衝突的職務或責任領域加以區隔。

(3) 資訊安全總負責人應對資安充分支持及承諾：確立保護公司的資訊安全的支持及承諾，將主導組織資安推動的方向，並將有限資源進行最大化發揮及整合，以主導組織資安推動的有效性及效益。例如聘請資安專責人員，或將部分資安維護及健檢事宜外包給資安廠商。

(4) 資訊安全總負責人應對於服務提供之資安給予充分支持：資訊安全總負責人應對服務提供之資安，給予充分支持。系統商提供資訊服務時，應重視公司客戶的資訊安全，以避免客戶的消費者之個資遭外洩，因此高階管理者，應於公司服務政策中確立，提供安全的資訊服務，是公司服務提供的重要事項，並對於公司提供資訊服務時，建構資安的資源提供支持。（系統商進階建議）

(5) 高階管理者宜提供資安訓練之資源：特別留意的是，每位員工若能對於資安觀念正確，認知自己為守護資安的重要一環，將是資安成功的關鍵。因此管理階層宜考量在資安相關訓練的投資，並且教育每位員工瞭解最佳的行事方式及技術知識。

2. 內部營運之資訊安全管理制度

公司應考量營運時所面對的內外部議題，建立一個符合公司目標的資訊安全政策及資訊安全目標，資訊安全政策並應以書面敘明。另外，亦要能識別資訊安全風險並予以對應。

（二）技術防護面

技術防護面分別有「資訊安全作業與保護」、「網路安全防護」、「電腦安全防護」、「資訊系統開發資安防護」、「資料安全管理」、「系統存取控制」、「系統維護」，以及「人員資安認知」等面向，以下分別簡介之：

1. 資訊安全作業與保護

公司應盤點公司的資訊系統，並確立系統作業流程與責任所需之控管方法，以確保資訊處理設施能被正確與安全操作。

實際行動則可透過以下方式執行：

(1) 資訊系統與設備盤點：公司應針對內部電腦及資訊系統，以及儲存客戶之消費者個人資料之系統或設備進行盤點。

(2) 確立系統作業流程的控管方式：系統作業流程可包含涉及變更時之變更控制方法、容量管理、開發測試與運作環境的分隔等。相關控管方法可包含：防範惡意程式的方法、備份以防範資料損失、紀錄系統更新、辨認判斷系統檔案異動之方式、存錄與監控系統檔案異動以記錄事件或留存證據、確保作業系統完整性、防範技術脆弱性等。

2. 網路安全防護

公司應於資訊安全政策文件中敘明為保護網路安全所採取之必要措施，以保護公開網路上的應用服務，並避免詐騙行為、契約

爭議及未經授權的存取與修改。

實際行動則可透過以下方式執行：

(1) 建立惡意中繼站黑名單（C2 Server）：利用惡意中繼站黑名單，即可幫助阻擋試圖進入網路的惡意參與者。市面上現有的惡意 IP 黑名單皆可參考利用，包含：行政院技服中心、企業內部蒐集之黑名單、國際即時黑名單列表（RBL）或、DNS 黑名單列表（DNSBL）等。

(2) 網路設備紀錄檔（log）分析：內部對外開放服務連線、內對外連線事件、異常高傳輸量情形、非上班時間之連線情形、內部是否有黑名單連線情形等。

(3) 流量封包側錄：網路封包異常連線、異常 DNS Server 查詢、惡意 IP、內部連接中繼站等符合網路惡意行為的特徵。

(4) 加強縱深防禦：透過資安設備保護內部連線安全，包含安裝 IDS/IPS、WAF、建立 DMZ 緩衝區、垃圾郵件或病毒過濾閘道等。

(5) 企業網段管理：重要系統網段獨立測試、正式環境網段與開發測試網段分離、測試平台禁止真實資料使用。

(6) 定期網頁弱掃、滲透測試：建議至少 1 年進行一次。

3. 電腦安全防護

公司應於資訊安全政策文件中敘明為保護內部電腦安全所採取之必要措施，以防範惡意程式、防範資料損失、確保作業系統完整性、防範技術脆弱性等。

實際行動則可透過以下方式執行：

(1) 關閉未使用服務或具風險之 Port：

- 在不影響服務正常運作的情況下，建議 TLS 可升級至最新版，並關閉 TLS 舊版本。
- FTP 應升級為 SFTP，並關閉 FTP。
- Telnet 應升級為 ssh，並關閉 Telnet。

(2) 密碼政策實施：參考行政院技服中心標準[15]，系統伺服器密碼應採取強密碼，最少 12 碼；包含英文大寫、英文小寫、阿拉伯數字、特殊符號；密碼更新至少 90 天更新應定期更換密碼，且不可與前 3 次使用過的密碼相同；密碼鎖定原則（密碼輸入錯誤達 5 次後，應至少 15 分鐘內不允許該帳號及來源 IP 繼續嘗試登入，避免遭暴力破解）；建議採用圖形驗證碼機制；密碼重設機制應採取先發送一次性且有時效性的憑證（token），有效回傳後才允許重設密碼。

(3) 建立系統及資料備援：儲存客戶個人資料檔案之媒體與資料，建立備份或備援機制。

(4) 定期主機弱掃、惡意程式檢測：建議至少 1 年進行一次。

(5) 定期軟體更新：定期檢視作業系統、防毒軟體、辦公軟體及應用軟體等之更新狀態。

4. 資訊系統開發資安防護

傳統程式開發的 SDLC 流程，未將資安考量進去。現在則將資安意識加入，成為 SSDLC 流程作為標準。因此，資訊安全政策文件應特別敘明資訊系統開發之程序與責任，以及相關控管方法，以確保資訊處理設施能被正確與安全操作。

實際行動則可透過以下方式執行：

(1) 設計階段（Design）：於設計階段（Design）考量資安威脅，應分析程式對外服務或內部登入於資安構面是否有風險，須於「威脅建模」(Threat Modeling)逐一列出，並討論解決方式。例如對外網站服務的資安威脅可參考 OWASP TOP 10（十大網路應用系統安全弱點），於設計階段考量資安威脅。

(2) 開發實作階段（Implementation）：應避免常見弱點及發展

---

[15] 行政院國家資通安全會報技術服務中心，《109 年政府資訊作業委外資安參考指引(修訂)v6.1_1100801》，〈附件 3 附錄 1 政府 Web 網站委外安全注意事項與安全檢核表〉，頁 1-9，https://download.nccst.nat.gov.tw/attachfilecomm/109%E5%B9%B4%E6%94%BF%E5%BA%9C%E8%B3%87%E8%A8%8A%E4%BD%9C%E6%A5%AD%E5%A7%94%E5%A4%96%E8%B3%87%E5%AE%89%E5%8F%83%E8%80%83%E6%8C%87%E5%BC%95(%E4%BF%AE%E8%A8%82)v6.1_1100801.rar （最後瀏覽日：2021/12/20）。

控制措施。例如：透過 HTTPS 傳輸加密、對稱或非對稱式加密資料庫。

(3) 驗證測試階段(Verification)：包含源碼檢測(靜態分析)、弱點掃描(動態分析)、滲透測試(動態分析)。

(4) 部署維運階段 (Deployment & Maintenance)：透過版本控制工具，掌握版本是否為最新版，並隨時更新版本、修補漏洞，以維持版本的最佳化。

5. 資料安全管理

系統商對於提供資訊服務，所涉及委託系統商之客戶的消費者資料，應提出保護資料完整性、機密性及正確性的方法。實際行動則可透過以下方式執行：(系統商進階建議)

(1) 資料傳輸

IT 系統遠端存取連線軟體需升級至企業版本，並將 SQL(結構化查詢語言) 更新至最新版，以降低可能存在的資安漏洞。

系統商透過 API 傳輸個資時，可將個資作有效之加密或隱碼遮罩，以防不幸發生個資外洩時，減少可被識別的資訊。系統商透過 API 接受個資時，亦可要求提供個資者將個資最小化，並作有效之加密或隱碼遮罩後再進行傳輸。

(2) 資料庫防護

A. 系統內採用加解密機制存取設定資料，並將資料庫、資料表個資採用加解密機制存取資料，並也增設存取 log 紀錄。

B. 個資密鑰與資訊系統資料區隔存放於不同位置。

6. 系統存取控制

公司應於資訊安全政策文件中敘明所採取的系統存取控制管理，以防止系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，並確保其機密性、完整性及可用性。

實際行動則可透過以下方式執行：

(1) 加強帳號註冊或註銷等權限管理：帳號最低權限原則（嚴格管控）、不共用帳號。

(2) 於系統中布建使用者身分配置程序。

(3) 管理使用者密碼資訊及特權存取權限應被限制與管理。

(4) 定期檢視使用者權限：隨著內部員工或合約關係（客戶或第三方）的轉變，移除或調整存取權限。

(5) 客戶登入後台之管控：協助客戶強化登入後台資料庫密碼複雜度，並採取多因子認證；限縮有權限進入後台系統（包含下載權限）之人數，但不共用帳密；縮短客戶帳號的登入閒置時間，並於閒置過久時強制登出。

7. 系統維護

(1) 不於非上班時間處理客戶突發問題：以確保所有系統操作皆由公司 IP 進行。

(2) 第三方資安健檢：定期由第三方資安廠商執行資安健檢，並佈署端點防護軟體。

(3) 發現系統弱點列表及控制措施：自主及尋求第三方協助發現的資訊服務系統或網站平台的弱點列表及控制措施，並提出預防或避免攻擊之作法可供線上驗證。

8. 人員資安認知

讓資安成為每一位同仁日常工作中的一環，將是資安成功關鍵。因此公司應透過教育訓練提升員工之資訊安全認知，並於政策文件中敘明資安教育訓練之規劃，包含實施頻率、教育訓練內容(例如：定期更新的組織政策或程序)、及要求員工接受訓練等情形。

實際行動則可透過以下方式執行：

(1) 人員資安職能訓練：可參考政府機關資安職能訓練發展藍圖，透過策略面、管理面、技術面等內容，安排共通訓練、基礎訓練及進階訓練等不同階段的訓練，辦理至少 1 年辦理一次人員資安職能訓練。

(2) 定期電子郵件社交工程演練：每 6 個月至少一次電子郵件社交工程演練，包含收信時不打開可疑信件、瀏覽網頁時不隨意點選可疑連結等，加強員工基本資安意識。

（三）作業流程面

如何做到上述技術面的內容、操作頻率、如何持續操作，就有賴作業流程面的管理。

1. 控制措施

參考 ISO/IEC 27001：2013 資訊安全管理系統之附錄 A，共有 14 個控制領域、35 個控制目標，以及 114 個控制措施。

控制領域依序包含：資訊安全政策、資訊安全組織、人力資源安全、資產管理、存取控制、密碼學、實體及環境安全、操作安全、通訊安全、系統獲取開發及維護、供應者關係、資訊安全事故管理、資訊安全持續、遵循性等 14 個項目。

2. 資訊安全管理的四階文件

可透過以下四階的文件作業，達成作業流程面的管理。

(1) 第一階文件：安全手冊

最高的指導文件在企業資訊安全管理為「安全手冊」內容，包括「資訊安全政策」或國際標準（例如 ISO 27001）之「適用性聲明」等。

(2) 第二階文件：管理辦法

第二階文件是資訊安全的「管理辦法」，將企業資訊安全管理制度文件化。例如：密碼管理辦法。

(3) 第三階文件：作業程序

第三階文件是「作業程序」，規定標準作業細節。例如：密碼轉換及報備作業管理程序、備份作業管理程序、門禁安全作業程序等。

(4) 第四階文件：紀錄表單

最底層的文件是作業流程中實際作業的「紀錄表單」，例如：辦公室安全檢查表、資訊設備攜出表等。

（四）遵循性

檢視個資及資安法令規範，以及於契約上釐清系統商本身與客戶或第三方之責任，避免違反相關法規（如個資法、客戶之主管機關訂定之相關法規等）及契約義務之要求。

1. 法規要求事項之識別

系統商應遵守「個人資料保護法」、「個人資料保護法施行細則」、「製造業及技術服務業個人資料檔案安全維護計畫管理辦法」。

另外，由於系統商係受客戶委託提供資訊系統服務，因此依據個資法第 4 條規定，系統商受委託而於系統蒐集、處理、利用個人資料時，視同客戶之行為，系統商因此也需要遵守客戶之主管機關相關法令規範。（系統商進階建議）

2. 契約要求事項之識別

系統商受委託建置、維運、維護系統，當這些資訊系統發生資安事故時，原因通常多重且複雜，起因有可能發生在系統商端，也可能來自客戶端，甚至可能發生於租賃第三方的雲端主機。因此對於系統商，應於訂定契約釐清系統商本身與客戶或第三方之資安責任，例如下列事項：（系統商進階建議）

(1) 定義所提供 ERP 服務的安全使用環境

於資訊安全文件中敘明資訊服務系統的安全使用環境，應配合採行哪些資訊安全配套措施或工具，以及資料透過 API 傳輸及存取過程之資安防護策略。

(2) 系統商之委託客戶義務

敘明客戶應備有資訊服務系統的安全使用環境、要求客戶盡資料保護責任。

例如：定期更新各式系統及軟體版本、配合加裝指定之資訊安全配套措施或工具、客戶自建伺服器者之連接加密等級、客戶之電腦設備不可安裝非法軟體、避免多人共用後臺登入之帳密、

離開電腦或下班時應從後臺登出、定期且頻繁針對登入後臺的電腦使用防毒軟體掃毒、上傳資料至系統前應就資料進行惡意程式偵測、定期做社交工程教育宣導及演練等。

(3) **系統商端義務：**

敍明系統商應備有資訊服務系統的安全使用環境，以遵循個人資料保護法要求的個資安全維護措施。

例如：確保網頁安全（SSL 加密）、應設計具加密功能的通道使客戶傳輸機敏資料、應設計傳輸機敏資料時隱碼（遮罩）不必要資訊、得管控客戶存取權限、定期做社交工程教育宣導及演練等。

(4) **租用雲端主機時應釐清責任：**

若系統商或客戶有任何一方，透過第三方業者租賃雲端主機或雲端儲存空間者，應在契約中清楚釐清連接架構。並確認哪一方應負擔資料存放和保護管理責任。

（五）證據保存面

公司應落實使用紀錄、軌跡資料及證據等內容的保存，包含以下執行方式：

1. **導入日誌分析系統與事件反應機制**：用以作為存錄與監控，以識別、蒐集、獲取及保存可作為證據之資訊，可逐日列舉分析紀錄。
2. **使用紀錄及軌跡資料證據保存：**執行資訊安全管理措施時，至少保存以下紀錄：(1)資料使用紀錄；(2)自動化機器設備之軌跡資料；(3)落實執行資訊安全管理措施之證據。
3. **討論紀錄：**公司任何優化資安政策程序之討論會議，宜製作書面紀錄以為佐證。

第四章 個人資料保護暨資訊安全檢查（CHECK）

為因應個資事故之危害風險、個資法遵成本及資安要求等營運風險，企業組織應於事故發生前（事前）做好維護措施、事故發生時（事中）採取應變措施、事故發生後（事後）採取修補措施。

本章主要說明事前之平時維護措施之檢查部分（參下圖 7）。

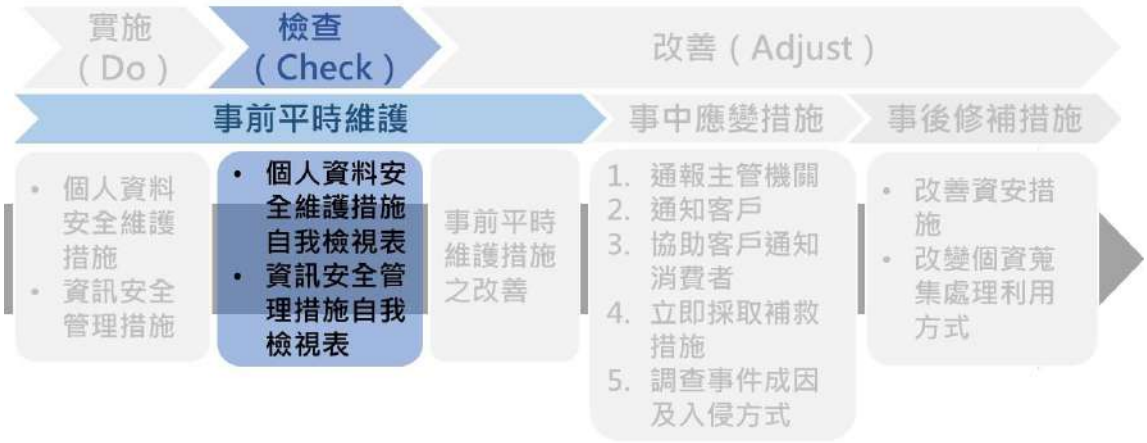

圖 11 因應風險應採取之措施流程圖－事前檢查
資料來源：本指引自製

系統商應就個人資料保護暨資訊安全平時維護措施的建構和實作等實施內容，定期進行以下檢查措施：

1. 平時自我檢查或內、外部稽核：

(1) 自我檢查及內部稽核

系統商可利用本指引**附錄一「系統商個人資料安全維護措施自我檢查表」**，以及**附錄二「系統商資訊安全管理措施自我檢查表」**，進行個人資料檔案安全維護及資訊管理管理之平時自我檢查或內部稽核，以檢查執行狀況。

自我檢查或內部稽核頻率，1 年至少 1 次為佳。個資專員並應規劃、執行針對全公司進行的自我檢查或內部稽核，並於稽核時紀錄所有過程。若內部稽核人員若取得稽核資格更佳。

(2) 外部個資安全稽核機制

若欲展現公司確實具有良好的個資安全維護能力，可進行外部稽核機制，委請第三方驗證機構，依據個資法相關法規及 BS 10012、ISO 27701 等國際標準進行驗證稽核。

資安方面，可委託外部第三方進行資安稽核、資安驗證（例如 ISO 27001），或委託資安公司進行資安健檢並提出檢測報告。

2. **回報給管理階層審查：**系統商負責自我檢查、內部稽核的人員，或委請的外部稽核人員，應將自我檢查或執行內外部稽核之結果，回報給個資保護及資安總負責人審查。

3. **立即矯正及更新個人資料保護暨資訊安全平時維護措施：**系統商應將檢查、稽核等活動發現的缺失立即矯正，以及將矯正措施內容更新於個人資料安全維護措施及資訊安全管理措施之中。

第五章 個人資料保護暨資訊安全改善（ADJUST）

為因應個資事故之危害風險、個資法遵成本及資安要求等營運風險，企業組織應於事故發生前（事前）做好維護措施、事故發生時（事中）採取應變措施、事故發生後（事後）採取修補措施。

本章說明個人資料保護暨資訊安全的改善，為因應風險改善的三階段措施，一為事前平時維護程序中，檢查後的改善；另一為當危害風險（個資事故）不幸發生時，系統商於事中之應變措施，三為危害風險（個資事故）事後之修補措施（參下圖 8）。

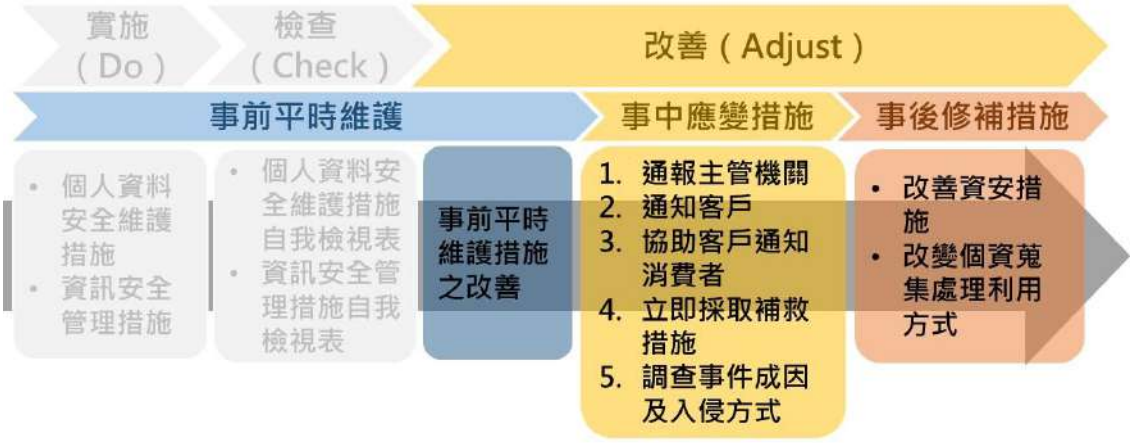

圖 12 因應風險應採取之措施流程圖－事中及事後
資料來源：本指引自製

一、事前平時維護措施之改善

系統商於內部自我檢查、內外部稽核等活動中所發現的缺失，宜透過以下方式，採取立即矯正措施：

1. 找出缺失之原因，以及評估是否可有類似的缺失存在，或之後可能發生缺失的項目。
2. 評估消除缺失項目所須採取的措施，並實際採取該些措施。
3. 審查所有已採取的矯正措施的有效性。
4. 將矯正措施更新於個人資料安全維護措施及資訊安全管理措施中。
5. 將缺失原因、所採取之矯正措施、採取措施的過程、採取措施的結

果、更新於個人資料安全維護措施及資訊安全管理措施的內容皆已文件化方式保存，做為參考依據及證據。

二、事中應變措施

當某企業組織發生個資事故(例如個資外洩)時，應立即進行以下措施：

（一）通報主管機關

依《製造業及技術服務業個人資料檔案安全維護管理辦法》第 6 條規定：

1. 通報時點：知悉發生事故 72 小時內。

2. 通報條件：業者遇有消費者個人資料安全事故，將危及其正常營運或大量當事人權益者。

3. 通報對象：業者應通報經濟部，或通報地方政府時副知經濟部。

4. 通報內容：事件發生種類、外洩大略筆數、發生原因及事件摘要、採取的因應措施、通知當事人的時間和方法。

通報方式宜以發函方式（紙本公文或電子公文皆可），並以「經濟部」為受文者，通知主管機關。函文內容可將前述通報內容以文字條列表述，亦可使用「通報紀錄表」。本指引提供通報紀錄表格式範例如下：

表 2 經濟部所管業者個人資料侵害事故通報與紀錄表

經濟部工業局所管業者個人資料侵害事故通報與紀錄表	
製造業或技術服務業者名稱 ○○○有限公司 **通報機關** 經濟部工業局	通報時間：○○○年○○月○○日　○○時○○分
	通報人：○○○　　簽名(蓋章)
	職　稱：○○○
	電　話：○○○
	Email ：○○○
	地　址：○○○
事件發生時間 註1：實際發生時間如填	實際發生時間：○○○年○○月○○日 ○○：○○ 知悉發生時間：○○○年○○月○○日 ○○：○○

<table>
<tr><td>寫「不明」者，請接續註明知悉個資外洩之時間</td><td colspan="2"></td></tr>
<tr><td rowspan="6">事件發生種類
註2：若為個資外洩，請勾選「竊取」及「洩漏」
註3：尚無法掌握侵害筆數時請寫「目前不明」</td><td>■竊取</td><td rowspan="3">個資侵害之總筆數(大約)
○○○筆</td></tr>
<tr><td>■洩漏</td></tr>
<tr><td>□竄改</td></tr>
<tr><td>□毀損</td><td rowspan="3">□一般個資 ○○○ 筆
□特種個資 ○○○ 筆</td></tr>
<tr><td>□滅失</td></tr>
<tr><td>□其他侵害事故</td></tr>
<tr><td>發生原因及事件摘要
註4：請簡要敘述目前掌握的即時情況即可，尚不須填寫詳細確切原因</td><td colspan="2">例：駭客利用境外IP發動攻擊，在系統○○○處植入木馬程式，竊取消費者資料，導致個資外洩</td></tr>
<tr><td>損害狀況
註5：請簡要敘述目前掌握的情況即可</td><td colspan="2">例：○○○年○○月至○○月期間出現多起包含「○○」等○○間客戶網站資料外洩。截至○○○年○○月至○○月止，已掌握○○○筆詐騙通報案</td></tr>
<tr><td>個資侵害可能結果
註6：例如利用個資進行電話詐騙、盜刷信用卡等</td><td colspan="2">例：利用個資進行電話詐騙、盜刷信用卡</td></tr>
<tr><td>擬採取之因應措施
註7：請簡要敘述目前已採取和準備採取之措施即可</td><td colspan="2">例：
1.立即採取補救措施：搜尋及刪除惡意程式、監控後台執行、控管前台風險（阻擋惡意IP、雙因子驗證、建立新的API過濾器)等
2.徹查事件原因：進行資料庫log查詢分析、執行弱點掃描及測透測試找出弱點等
3.協同客戶因應：自○○月○○日起發送事件通知及後續措施予客戶；配合客戶發送通知簡訊及email給消費者
4.擬採取之持續改善措施：
(1)變更系統中資料修改權限並加上二次驗證
(2)個人機敏資料遮罩
(3)增加帳號登入密碼定期強迫更新機制</td></tr>
</table>

擬採通知當事人之時間及方式 註8：可簡要敘述如何通知客戶；或者如何協助客戶通知客戶之消費者	例：配合電商客戶發送防詐騙簡訊及電子郵件。並協助客戶在其官網及社群網站揭露防詐騙訊息。
是否於發現個資外洩時起算七十二小時內通報 註9：逾72小時通報主管機關者，請簡述延遲通報理由；僅報警者不屬於已通報主管機關	例： ■是　　□否，理由：

資料來源：經濟部工業局

（二）通知客戶

系統商協助客戶代管主機或儲存資料時，因而保有消費者個資，因此當知悉消費者個資因資安事故有外洩等情形時，應基於與客戶的契約關係，先立即通知客戶業者。方式不限，能立即、適當、訊息充足，使客戶清楚知悉即可。

另外，應立即要求客戶更新系統、更改密碼、進行惡意程式偵測、弱點掃描、掃毒等。

（三）協助客戶通知其消費者

通報當事人部分，理論上應由與消費者直接接觸、蒐集消費者個資之業者（例如電商業者、私人醫院診所、私立學校、非營利組織等），依個人資料保護法為通知，不過系統商可能與客戶基於契約關係，或受客戶另外委託，協助客戶代為通知消費者。

通知消費者的內容，應明確向消費者表示個資遭竊取、已採取的因應措施、通知當事人的時間和方法。若僅寄發提醒防詐騙宣導的內容給遭個資外洩事故之消費者當事人，而未明確向其表示個資已遭外洩，可能會被認為不符個資法第 12 條之規定，而可能會受到個資法

第 48 條之處分。[16]應再留意的是，系統商雖受客戶業者委託，協助代為通知消費者，但通知內容是否合於個資法規定，最終仍應由客戶業者自行負責。

以下為《個人資料保護法》第 12 條[17]、《個人資料保護法施行細則》第 22 條[18]所規範的適當通知方式：

1. 通知時點：自知悉時起即應盡速通報。

2. 通知條件：業者遇有消費者個資被竊取、洩漏(個資外洩)或竄改、損毀、滅失之事故。

3. 通知內容：使當事人知悉個資遭竊取、已採取的因應措施、通知當事人的時間和方法。而非僅是防詐騙宣導。

4. 通知方式：以簡訊、電子郵件等其他足以使當事人知悉或可得知悉之方式。

（四）立即採取補救措施

應立即透過惡意程式偵測，或委請資安公司利用數位鑑識等方式，尋找惡意程式（病毒及木馬）並刪除之，立即止血以防止損害擴大。若損害層面過大，建議必要時可考慮先將涉及外洩客戶部分之系統伺服器暫停營運（停機）。

另外，應採取最基礎的停止損害措施，例如立刻限制國外 IP 存取、限縮客戶帳號存取權限等。

（五）調查事件成因及入侵方式

調查事件成因，應調查系統商提供的資訊系統本身及前台網站，以及協助客戶調查事件成因，並包含客戶委託之第三方業者與系統商所串接的傳輸資訊渠道（如 API 協定等）。

---

[16] 行政院訴願決定書院臺訴字第 1050183642、1050184074 號。

[17] 《個人資料保護法》第 12 條：「公務機關或非公務機關違反本法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人。」

[18] 《個人資料保護法施行細則》第 22 條：「本法第十二條所稱適當方式通知，指即時以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之。但需費過鉅者，得斟酌技術之可行性及當事人隱私之保護，以網際網路、新聞媒體或其他適當公開方式為之。（第 1 項）依本法第十二條規定通知當事人，其內容應包括個人資料被侵害之事實及已採取之因應措施。（第 2 項）」

調查事件及入侵方式，包含調取 log 查閱是否有異常 IP、透過資安健檢尋找後台系統及前台網站漏洞（包含原碼檢測、滲透測試、弱點掃描等）、研究駭客路徑找出其他可能成因（例如員工遭受社交工程攻擊並上當）等。

三、事後改善修補措施

當某企業組織發生資安事故（例如個資外洩）後，無論是否已調查出事件成因，都應立即進行以下修補措施：

（一）改善資安措施

若事件已調查出成因，透過已釐清之事件成因進行弱點漏洞修補、部分或全面改善系統資安防護措施等（例如系統架構變更、強化防火牆、傳輸渠道加密、資料庫加密等）。

若尚未調查出成因，則應全面建構縱深防禦平台資訊系統的控制措施，以面對不定期、持續性的網路惡意攻擊。

（二）改變個資蒐集處理利用方式

包含採取個資最小化措施（例如傳輸個資時遮罩隱碼）、改變個資蒐集內容、改變個資傳輸方式、改變個資儲存地點及方式等。

（三）重新評估與客戶間資安責任

評估客戶是否能承擔改善修補後的資安保護能力成本，重新以契約約定雙方資安責任，或者於客戶無力負擔時不再與該客戶續約，以免使系統商本身承受過多危害風險。

四、配合主管機關調查

依個人資料保護法第 22 條規定，中央目的事業主管機關認有必要或有違反個資法規定之虞時，得請相關人員為必要之說明、配合措施或提供相關證明資料。

經濟部工業局係資訊服務業之中央目的事業主管機關，於知悉有個資事故發生時，為瞭解所管業者與疑似個資外洩事件之關聯，將依前揭規定請系統商提供相關資料以利釐清問題事件發生之原因。一般於調查時，經濟部工業局會以發函方式，請系統商提供說明並備佐證資料，例示如下：

（一）個案分析報告

1. 與委託客戶間之關係：

   (1) 系統架構圖（例如：系統的網路架構圖、個資傳輸及存放地點架構圖等）及系統架構文字說明。

   (2) 貴公司對客戶之資安環境要求及相關權限控管。

   (3) 貴公司與客戶間之契約要求內容。

2. 個資外洩發生的可能原因。

3. 事件發生前所採行之平時資料維護措施。

4. 事件發生時所採取之應變措施。

5. 事件發生後所採行之改善措施。

（二）公司資安保護措施，重點如下：

1. 資料安全管理：如加密措施、對於備份資料之保護措施、保存與傳輸安全之維護措施等；如有涉及使用資訊系統者，亦應一併敘明資訊系統之安全維護措施，包括：防火牆或其他入侵偵測設備、防毒措施、系統與程式漏洞檢視與修補、使用者認證機制、異常存取資料行為之監控機制、系統測試之個資保護機制等。

2. 人員安全管理：如人員保密措施、存取權限之控制、人員離退時之資料返還等。

3. 設備安全管理：敘明對存有個人資料之紙本、磁碟、磁帶、光碟片、微縮片、積體電路晶片、電腦、自動化機器設備及其他媒介物（以下簡稱儲存媒介物），所採取之設備安全管理措施，包括對存放儲存媒介物之環境，所取之適當的之進出管制措施等。

4. 認知宣導及教育訓練：如舉辦宣導活動之形式、個資教育訓練之機制與頻率等。

為盡快釐清事故發生成因與責任，建議業者於落實各項措施時，應保存相關事證，以於主管機關進行調查時能夠清楚說明。函復主管機關之調查

時，常見需提供之佐證資料可參考附錄三。

另外，為促進國內資安事件情資分享，強化資安防禦體系，提升我國資安自我防護能量，以及使業者能即時掌握國內外重大資安事件，建議系統商加入「台灣 CERT/CSIRT 聯盟」會員。系統商可至「台灣電腦網路危機處理暨協調中心（TWCERT/CC）」網站首頁[19]，按下「申請加入聯盟」按鈕申請加入會員。

[19] 台灣電腦網路危機處理暨協調中心(TWCERT/CC)，https://www.twcert.org.tw/tw/mp-1.html（最後瀏覽日：2021/12/20）。

第六章 安全維護措施常見問題案例

本指引特別摘錄系統商進行個資安全維護措施時，在平時維護、採取應變措施及修補措施時常見的問題，提供建議供各業者參考。

一、事前：忽略資料庫應區隔網段的重要性

（一）範例

A 公司銷售前後台系統，由客戶自行決定系統主機放置方式，A 公司另有提供主機代管服務。某日起，由 A 公司代管系統的數家客戶，連續發生多起消費者個人資料外洩情形。A 公司除立即報案外，也通報其主管機關及協助機構客戶之通知其會員。並立即調查個資外洩的原因，發現網路架構有以下情況：

1. 雖然有獨立的 AP services、DB services、網頁服務（Web Server）、測試區，但都在同一網段，並共同接入同一部網路交換器（Network switch）。
2. 部分加密 Key 包含在程式。

（二）建議：資料庫區隔

1. **AP services 跟 DB services 宜區隔網段**
2. **建立 DMZ 非軍事區**

宜將網頁服務（Web Server）移出 Switch 之外，並於網路與防火牆之間建立 DMZ（Demilitarized zone，非軍事區）放置 Web Server，使外部流量不會接觸 AP services、DB services 及測試區。

3. **加解密的 KEY 不綁在程式內**

加解密的 KEY 綁在程式裡面，有一定風險，因為放在程式後通常不會再變更，加解密的方式建議改用參數、變數的方式處理，以方便時常變更密碼，增加維護性。此外，個資密鑰與資訊系統資料建議區隔存放。

二、事前：疏於更新 API 交換協議資安規格

（一）範例

B 公司提供的電商開店平台系統，利用 Open API 使電商客戶可與第三方企業資源規劃系統（ERP）介接。某日起，B 公司與某 ERP 系統公司之數家共同電商業客戶，連續發生多起電商網站消費者個人資料外洩情形。

（二）建議：更新 API 交換協議資安規格

1. 定期更新 API 交換協議資安規格

應定期更新，修改與各客戶端 ERP 系統串接電商客戶使用的網路電商平台業者之 API 時，所使用的交換協議資安規格。

2. API 傳輸之資料宜隱碼遮罩

ERP 系統接收電商平台提供之訂單內容，個資部分已部分遮罩。

3. API 加裝安全驗證機制

加裝安全驗證機制，排除不在安全值內的連線，或示警不合安全性需求的連線，以強化系統操作安全性及自身產品責任。

三、事中：缺乏事故管理程序而沒有立即停損

（一）範例

C 公司向電商客戶銷售企業資源規劃（ERP）系統，使客戶能於其主機伺服器內安裝，C 公司會提供售後維修服務。電商業客戶可透過主機伺服器內的 API 程式，串接電商網站後台系統，將資料從後台系統存入 ERP 系統。

某日起，C 公司的數家電商業客戶，連續發生多起電商網站消費者個人資料外洩情形。C 公司雖有主動聯繫電商客戶，釐清可能問題，但由於 ERP 系統架構所串接的第三方業者眾多，個資外洩原因可能另外存在於網路、平台、雲端服務及電商業者使用行為各環節，因此 C 公司未能事件外洩根本原因未能被完整分析，致使外洩仍持續一段時間。

（二）建議：建立事故管理程序

宜建立事故管理程序（事故反應機制），以確保嗣後對事故能做

出迅速、有效及有程序的偵測及回應，減少事中反應所耗之時間。

1. 立即通知相關部門

例如事故發生時，立即通知相關部門（包含管理階層、客戶服務、資訊部門及法務部門）採取因應措施。除了客戶服務通知客戶事件發生情形、法務部門立即報警及通報主管機關之外。

2. 資訊部門立刻釐清事故原因並防堵

此外，資訊部門應立即就事故網站偵測惡意程式、調閱伺服器 IP 存取紀錄，以及透過資訊服務系統之網路架構、服務模式（與客戶端、系統伺服器端之串接關係）等，分析釐清事故原因、事故來源數量與發生位置，以立即將資安漏洞防堵，避免個資持續外洩。

四、事後：僅改變蒐集及存放資料的方式而忽略修補漏洞

（一）範例

D 公司受電商業者委託，提供公版前台網站並維護後台系統，後台系統可供電商客戶之工作人員登入，查閱網站品項、購買者資料、報表等資訊。

某日起，D 公司陸續收到電商客戶反映其消費者收到詐騙電話。除了報警及寄發防詐騙簡訊給電商客戶的消費者等通報外，D 公司也立即將留在本地資料庫的消費者帳號個人資料全數刪除，並改為「社群帳號登入」，重新蒐集消費者資料，並儲存於外部雲端封閉式系統，電商客戶透過 API 接收消費者資訊已部分隱碼。不過，一段時間後，D 公司系統又發生個資外洩。

（二）建議：建構縱深防禦平台資訊系統的控制措施

1. 仍應持續釐清事件成因並修補漏洞

建議仍應持續釐清事件成因，並將釐清成因所發現之漏洞進行修補，而非僅是改變蒐集及存放資料的方式，而忽略修補本已存在的漏洞。

2. 對 API 進行定期弱掃

另外，雖然電商透過 API 傳送消費者資訊雖已部分隱碼，若不

幸又發生資料外洩時，資訊量雖可能不足以被詐騙集團編造情境，但表示 API 傳輸渠道仍可能產生漏洞，因此仍有對 API 進行定期弱掃的必要。

3. 建構縱深防禦平台資訊系統的控制措施

由於原始資料仍存在於外部雲端封閉式系統由於外部雲端，即使最先進的雲端空間都還是有可能存在新的漏洞，因此仍應持續以系統性的方法，建構縱深防禦平台資訊系統的控制措施，以面對網路的惡意攻擊。

五、事後：修補時忽略客戶使用後台系統的缺失

（一）範例

E 公司受電商業者委託，提供前台網站並維護後台系統，後台系統可供電商客戶之工作人員登入，查閱網站品項、購買者資料、報表等資訊，並使電商客戶之工作人員可進行網站設計修改、訂單讀取修改等功能。

某日起，E 公司陸續收到電商客戶反映其消費者收到詐騙電話，E 公司立即報警及寄發防詐騙簡訊給電商客戶的消費者等通報，並立即全面重新建立新的主機環境。此外，透過帳密及手機驗證等雙因子驗證作法管控登入後台權限，並限定台灣 IP 始可登入。後台的消費者個資，已透過系統在批次處理清單時，將消費者姓名或針對電話、地址部份遮罩。

惟數月後，E 公司又發生個資外洩事情，疑似是客戶使用後台系統習慣不佳造成。

（二）建議：強化客戶使用系統之管制

全面重新建立新的主機環境只能解決程式弱點所衍生之資料安全風險，因此仍建議應強化以下客戶使用系統之管制措施：

1. 強化客戶資料存取之權限控管

強化資料存取之權限控管，例如限縮有權進入系統及下載權限之人數、要求上傳資料前應先偵測惡意程式、應限縮客戶上傳圖片及資料的權限、對資料庫的存取權限做分級等。

2. 強化客戶周邊系統的管制

強化周邊系統的管制，例如縮短客戶帳號登錄閒置時間並使其強制登出、要求客戶定期對電腦進行掃毒等。

3. 強化防火牆

鑒於客戶上傳資料習慣不佳，建議新加裝具有「網路應用程式防火牆」（Web Application Firewall）功能，以及能有效阻擋「Word攻擊」及「圖像隱碼術」（Steganography）的防火牆。

附錄

附錄一：系統商個人資料安全維護措施自我檢查表

表 3 系統商個人資料安全維護措施自我檢查表

系統商個人資料安全維護措施自我檢查表				
公司名稱：		檢查時間：		檢查人：
編號	檢查項目	系統商進階	適用情形	檢查情形說明
1. 配置管理之人員及相當資源				
1.1 配置個資保護總負責人				
1.1.1	由高階管理者擔任個資安全總負責人 可由總經理、代表人擔任、副總經理級或資安長級擔任		□適用 □不適用 說明：	□由_____(職位)擔任
1.1.2	個資安全總負責人應確保有關資安角色與職權之分配與傳達		□適用 □不適用 說明：	□制定公司內部權責 □統籌各部門、協調與推動資安防護相關事宜及所需之資源 □檢驗所有資訊保護的防護措施的正確完成執行
1.2 配置個資管理專員				
1.2.1	配置管理人員（一位或以上）		□適用 □不適用 說明：	□有配置管理人員辦理個資安全維護事項之落實 □（建議）公司總管理人員為專責人員
2.界定及盤點個人資料之範圍				
2.1 蒐集處理利用個人資料之告知				
2.1.1	「蒐集處理利用個人資料」告知義務 除有免告知事由，應對資料當事人踐行告知「當事人得行使權利」之義務		□適用 個人資料保護法第 8 條	□蒐集、處理、利用個人資料時有皆盡告知義務
2.2 界定個人資料之範圍				
2.2.1	蒐集、處理、利用個資之		□適用	□員工

	對象		製造業及技術服務業個人資料檔案安全維護管理辦法第 4 條	□客戶承辦人 □上下游供應商承辦人 □受委託處理個資 □維修時接觸個資 □其他：
2.2.2	界定個人資料範圍 建議使用法務部訂定之「個人資料保護法之特定目的及個人資料之類別」敘明所蒐集個資之特定目的及類別		□適用 製造業及技術服務業個人資料檔案安全維護管理辦法第 4 條	□敘明界定之特定目的及個資類別 □使用法務部訂定之「個人資料保護法之特定目的及個人資料之類別」敘明目的類別 □其他：
2.3 個人資料盤點				
2.3.1	計算及呈現個人資料筆數 建議可使用「分析個資流程」方式		□適用 □不適用 說明：	□清查各作業流程表單及紀錄，辨識、歸納、整理成個人資料檔案 □使用個人資料盤點表檢視個資檔案，確認檔案名稱、保有依據、特定目的、個資種類 □使用個人資料盤點表檢視個資檔案之生命週期過程內容及是否合法 □其他方式：
3.風險評估與管理機制				
3.1 風險評估				
3.1.1	系統或設備之風險評估	◎	□適用 □不適用 說明：	□評估公司內部電腦及資訊系統 □評估儲存客戶之消費者個資之系統或設備 □其他：
3.1.2	蒐集、處理、利用作業之風險評估 蒐集、處理與利用可能產生的各種作業情境及內容		□適用 製造業及技術服務業個人資料檔案安全維護管理辦法第 5 條	□加工（例如輸入、編輯、輸出、掃描等） □內部傳輸（例如 E-mail、網路伺服器） □外部傳輸（例如 E-mail、網路伺服器） □保管儲存（載體包含個

				人電腦、資料庫、主機伺服器)(不當存取、個人電腦遭外部攻擊) □廢棄(例如刪除、資料銷毀不夠落實致外洩) □其他：
3.2 風險管理				
3.2.1	風險管理 針對風險評估結果提出預定或已採取之具體風險管理措施或風險處理對策		□適用 製造業及技術服務業個人資料檔案安全維護管理辦法第 5 條	□加工管理方式： □內部傳輸管理方式： □外部傳輸管理方式： □保管儲存管理方式： □廢棄管理方式： □其他：
4.事故之預防、通報及應變機制				
4.1 事故預防				
4.1.1	建立事故預防、通報(當事人及主管機關)及應變機制		□適用 □不適用 說明：	□建立機制 □以流程圖呈現 □至少一年一次事故演練並檢討
4.2 事故通報				
4.2.1	通報主管機關 敘明以下內容 通報時點：知悉發生事故 72 小時內 通報條件：業者遇有消費者個人資料安全事故，將危及其正常營運或大量當事人權益者。 通報對象：業者應通報經濟部，或通報地方政府時副知經濟部。 通報內容：事件發生種類、外洩大略筆數、發生原因及事件摘要、採取的因應措施、通知當事人的時間和方法。 延遲通報：無法於時限內通報或無法於當次提供通報內容中的全部資訊時，應附延遲理由或分階段提供。		□適用 製造業及技術服務業個人資料檔案安全維護管理辦法第 6 條	□通報時點： □通報條件： □通報對象： □通報內容： □延遲通報： □其他：
4.2.2	通知客戶業者及其消費者	◎	□適用	□通知客戶業者

	敘明以下內容 通知時點：盡速。 通知事由：業者遇有消費者個資被竊取、洩漏(個資外洩)或竄改、損毀、滅失之事故。 通知內容：使消費者知悉個資遭竊取、已採取的因應措施、通知當事人的時間和方法。 通知方式：以簡訊、電子郵件等其他足以使當事人知悉或可得知悉之方式。		個人資料保護法 第 12 條 契約關係	□協助通知消費者 □通知時點： □通知條件： □通知內容： □其他：
4.3 事故應變及矯正措施				
4.3.1	事故發生時應變 列舉發生時、發生後之可能做法或執行流程，包含降低、控制當事人損害之方式		□適用 □不適用 說明：	□建立做法或執行流程 □立即通報主管機關 □立即通知客戶 □協助客戶通知其消費者 □調查事件成因 □立即採取補救措施（尋找惡意程式等） □重新評估與客戶間資安責任 □其他：
4.3.2	事故發生後矯正 研議矯正改善措施之機制		□適用 □不適用 說明：	□建立做法或執行流程 □改善資安措施（必須採取） □改變個資蒐集處理利用方式（選擇採取） □其他：
5.內部管理程序				
5.1 個人資料之蒐集、處理或利用程序				
5.1.1	蒐集		□適用 □不適用 說明：	□敘明以何種方式蒐集之個人資料 □敘明如何向當事人告知蒐集之目的，或變更使用之目的 □敘明如何檢視蒐集是否符合個資保護相關法

				令要求的特定目的 □其他：
5.1.2	處理		□適用 □不適用 說明：	□敘明以何種方式處理 □敘明如何檢視處理個資時是否符合個資法所稱特定目的 □其他：
5.1.3	利用		□適用 □不適用 說明：	□敘明以何種方式利用及行銷 □敘明拒絕行銷時的後續處理機制為何 □其他：
5.1.4	特定目的已消失或期限已屆滿		□適用 製造業及技術服務業個人資料檔案安全維護管理辦法第 7 條第 9 款	□敘明以何種方式檢視 □敘明已消失或已屆滿後如何處理 □其他：
5.2 受理當事人行使權利之程序				
5.2.1	告知「當事人得行使權利」義務 除有免告知事由，應對資料當事人踐行告知「當事人得行使權利」之義務		□適用 個人資料保護法第 8 條第 1 項第 5、6 款	□告知當事人得依個資法第 3 條規定得行使之權利及方式 □告知當事人得自由選擇提供個人資料時不提供將對其權益之影響
5.2.2	受理程序 於個人資料安全維護計畫中敘明受理當事人行使權利之程序		□適用 □不適用 說明：	□建立受理當事人行使權利之程序 □使當事人知悉受理程序流程 □以文字使當事人知悉 □以流程圖使當事人知悉
5.3 國際／境外傳輸				
5.3.1	是否有國際／境外傳輸 公司之伺服器或資料庫位在我國以外之國家地區，則有個人資料為國際／境外傳輸之情形		□適用 □不適用 說明：	□有國際／境外傳輸 □傳輸地區： □傳輸方式： □無國際／境外傳輸
5.3.2	檢視是否受主管機關經濟部限制		□適用 製造業及技術服	□有檢視限制 □未檢視限制

			務業個人資料檔案安全維護管理辦法第 9 條 □不適用 說明：	
5.3.3	告知「個資有國際／境外傳輸」義務		□適用 製造業及技術服務業個人資料檔案安全維護管理辦法第 9 條 □不適用 說明：	□告知資料當事人，其個人資料會傳輸至我國以外地區處理、利用
5.4 委託他人蒐集、處理或利用個人資料之管理程序				
5.4.1	委託他人蒐集、處理或利用個人資料之管理程序		□適用 個人資料保護法施行細則第 12 條 □不適用 說明：	□有委託他人蒐集、處理或利用個人資料 □有對受託者進行個資安全維護之監督管理 □於契約中敘明個資安全維護責任之事項 □對受託者進行稽核 1 年至少 1 次等 □其他 □無委託他人蒐集個人資料之情形
5.5 業務終止後有關於個人資料之處理方式				
5.5.1	特定業務減少或終止		□適用 製造業及技術服務業個人資料檔案安全維護管理辦法第 14 條第 2 項	□建立業務項目終止時個資處理方式 □個資刪除之程序及佐證 □個資移轉之原因、對象、方法、時間、地點、受移轉對象得保有該個人資料之合法依據。 □使資料當事人知悉其個資被移轉至他公司 □使當事人能行使個資法第 3 條之權利
5.5.2	法人格消滅		□適用 製造業及技術服	□建立法人格消滅時個資處理方式

			務業個人資料檔案安全維護管理辦法第 14 條第 2 項	□個資刪除之程序及佐證 □個資移轉之原因、對象、方法、時間、地點、受移轉對象得保有該個人資料之合法依據。 □使資料當事人知悉其個資被移轉至他公司 □使當事人能行使個資法第 3 條之權利
5.5.3	個資移轉予其他法人		□適用 個人資料保護法第 9 條	□建立移轉個資處理方式 □個資移轉之原因、對象、方法、時間、地點、受移轉對象得保有該個人資料之合法依據。 □使資料當事人知悉其個資被移轉至他公司 □使當事人能行使個資法第 3 條之權利
6. 資料安全管理及人員管理				
6.1 資料安全管理措施				
6.1.1	基本資料安全管理措施		□適用 製造業及技術服務業個人資料檔案安全維護管理辦法第 8 條第 2 項	□資料加密機制 □對備份資料採取適當保護措施 □傳輸資料時採取適當保護措施 □使用者認證機制 □異常存取監控機制 □其他：
6.1.2	以資訊系統處理個資	◎（隱碼機制）	□適用 製造業及技術服務業個人資料檔案安全維護管理辦法第 8 條第 2 項	□防火牆 □防毒軟體 □弱點掃瞄及修補 □密碼及認證機制 □異常存取行為監控 □避免利用真實個資測試 □資訊系統變更時確保其安全性未降低 □定期檢查

				□個資（傳輸時）隱碼 □個資（於提供電子商務時）隱碼 □其他：
6.1.3	平台資訊系統檔案發生異動	◎	□適用 □不適用 說明：	□辨識、判斷異動 □採取補償措施 □留存平台系統的更新紀錄 □其他：
6.2 人員安全管理措施				
6.2.1	基本人員安全管理措施		□適用 製造業及技術服務業個人資料檔案安全維護管理辦法第 10 條	□人員保密義務約定 □人員進出管制措施 □人員保密措施 □人員存取權限之控制 □人員離退時之資料返還 □其他：
6.2.2	分散式管理或沒有固定辦公場所之人員安全管理措施	◎	□適用 □不適用 說明：	□人員存取紀錄 □資料返還紀錄 □其他：
7. 認知宣導及教育訓練				
7.1	內部員工教育訓練 訓練內容：個人資料保護相關法令之規定；所屬人員之責任範圍；本計畫各項管理程序、機制及措施之要求 頻率：敘明實施頻率，並至少於公司資安或個資政策更新時實施。 程序；訂定實施頻率；每次宣導或訓練時訂定主題、議程，且實施簽到、製作會議紀錄、課後評量機制		□適用 製造業及技術服務業個人資料檔案安全維護管理辦法第 11 條	□訓練內容： □訓練頻率： □訓練程序： □其他：
7.2	外部客戶認知宣導	◎	□適用 □不適用 說明：	□契約簽訂前向該客戶揭露其個人資料安全維護措施 □使客戶認知使用系統時所需安全環境

				□其他認知宣導措施：
8.設備安全管理措施				
8.1	基本設備安全管理措施		□適用 製造業及技術服務業個人資料檔案安全維護管理辦法第 12 條	□人員管理規範 □人員進出管制 □適當之保護設備或技術 □過期資料及軟硬體的處理方式 □其他：
9.使用紀錄、軌跡資料及證據保存				
9.1	使用紀錄及軌跡資料證據保存 至少五年：a.個人資料使用紀錄；b.自動化機器設備之軌跡資料；c.落實執行個人資料檔案安全維護計畫之證據		□適用 製造業及技術服務業個人資料檔案安全維護管理辦法第 14 條第 1 項	□個人資料使用紀錄 □保存 5 年 □保存____年 □自動化機器設備之軌跡資料 □保存 5 年 □保存____年 □落實執行個人資料檔案安全維護計畫之證據 □保存 5 年 □保存____年 □其他：
9.2	因業務終止而銷毀證據保存		□適用 製造業及技術服務業個人資料檔案安全維護管理辦法第 14 條第 1 項	□有紀錄銷毀方法、時間、地點及證明銷毀之方式 □有紀錄移轉原因、對象、方法、時間、地點及受移轉對象得蒐集該個人資料之合法依據 □其他：
10.資料安全稽核機制				
10.1	內部個資安全維護稽核機制		□適用 製造業及技術服務業個人資料檔案安全維護管理辦法第 13 條	□1 年至少____次檢查個資安全維護執行狀況 □內稽人員具合格稽核資格 □提出評估報告 □採行改善機制 □其他：

10.2	外部個資安全維護稽核機制		□適用 □不適用 說明：	□委請第三方稽核 □委請第三方驗證機構稽核 □其他：
11.持續改善措施				
11.1	持續改善措施		□適用 製造業及技術服務業個人資料檔案安全維護管理辦法第 15 條	□敘明未落實執行時應採取矯正預防措施 □敘明定期檢視或修正本計畫 □以 PDCA 持續改善 □其他履行方式： □其他：

資料來源：本指引自製

附錄二：系統商資訊安全管理措施自我檢查表

表 4 系統商資訊安全管理措施自我檢查表

系統商資訊安全管理措施自我檢查表				
公司名稱：		**檢查時間：**		**檢查人：**
編號	**檢查項目**	**系統商進階**	**適用情形**	**檢查情形說明**
1.營運管理面				
1.1 資訊安全權責				
1.1.1	由高階管理者擔任資訊安全總負責人		□適用 □不適用 說明：	□由_____(職位)擔任
1.1.2	資訊安全總負責人應確保有關資安角色與職權之分配與傳達		□適用 □不適用 說明：	□制定公司內部權責
1.1.3	資訊安全總負責人應對資安充分支持及承諾		□適用 □不適用 說明：	□支持及承諾事項：
1.1.4	資訊安全總負責人應對服務提供之資安給予充分支持	◎	□適用 □不適用 說明：	□支持及承諾事項：
1.1.5	高階管理者宜提供資安訓練之資源		□適用 □不適用 說明：	□提供資安訓練之資源
1.2 內部營運之資訊安全管理制度				
1.2.1	內部營運之資訊安全管理制度		□適用 □不適用 說明：	□考量並敘明營運時所面對的內外部議題 □制定政策，內容包含： - 資訊安全的目標 - 概要資訊安全原則的需求
2.技術防護面				
2.1 資訊安全作業與保護				
2.1.1	資訊系統與設備盤點	◎	□適用 □不適用 說明：	□內部電腦系統 □內部資訊系統 □儲存客戶之消費者個人資料之系統及設備

				□其他：
2.1.2	確立系統作業流程的控管方式 系統作業流程可包含涉及變更時之變更控制方法、容量管理、開發測試與運作環境的分隔等		□適用 □不適用 說明：	□防範惡意程式 □備份 □存錄與監控 □確保作業系統完整性 □防範技術脆弱性 □其他控管方法：
2.2 網路安全防護				
2.2.1	建立惡意中繼站黑名單		□適用 □不適用 說明：	□建立惡意中繼站黑名單
2.2.2	網路設備紀錄檔（log）分析		□適用 □不適用 說明：	□內部對外開放服務連線 □內對外連線事件 □異常高傳輸量情形 □非上班時間之連線情形 □內部是否有黑名單連線情形 □其他：
2.2.3	流量封包側錄		□適用 □不適用 說明：	□網路封包異常連線 □異常 DNS Server 查詢 □惡意 IP □內部連接中繼站 □其他：
2.2.4	加強縱深防禦		□適用 □不適用 說明：	□安裝 IDS/IPS □安裝 WAF □建立 DMZ 緩衝區 □垃圾郵件過濾閘道病毒過濾閘道 □其他：
2.2.5	企業網段管理		□適用 □不適用 說明：	□重要系統網段獨立測試 □正式環境網段與開發測試網段分離 □測試平台禁止真實資料使用 □其他：

2.2.6	定期網頁弱掃、滲透測試 建議每 1 年至少 1 次		□適用 □不適用 說明：	□網頁弱掃頻率：1 年至少 1 次 □滲透測試頻率：1 年至少 1 次
2.3 電腦安全防護				
2.3.1	關閉未使用服務或具風險之 Port 在不影響服務正常運作的情況下，建議 TLS 可升級至最新版，並關閉舊版本		□適用 □不適用 說明：	□關閉未使用的 TLS 舊版本 □關閉 FTP，升級為 SFTP □關閉 Telnet，升級為 ssh □其他：
2.3.2	密碼政策實施		□適用 □不適用 說明：	□公司端伺服器最少 12 碼 □使用者端伺服器最少 8 碼 □英文大寫、英文小寫、阿拉伯數字、特殊符號至少四選三 □密碼更新至少 90 天更新 □訂定密碼鎖定原則： □其他：
2.3.3	建立系統及資料備援		□適用 □不適用 說明：	□建立系統備援 □建立資料備援
2.3.4	定期主機弱掃、惡意程式檢測 建議每 1 年至少 1 次		□適用 □不適用 說明：	□主機弱掃頻率：1 年至少 1 次 □惡意程式檢測頻率：1 年至少 1 次
2.3.5	定期軟體更新 檢視作業系統、防毒軟體、辦公軟體及應用軟體等之更新狀態		□適用 □不適用 說明：	□更新頻率： □更新軟體內容包含：
2.4 資訊系統開發資安防護				
2.4.1	設計階段（Design） 對外網站服務的資安威脅可參考 OWASP TOP 10（十大網路應用系統安全弱點），於設計階段考量資安威脅	◎	□適用 □不適用 說明：	□分析程式對外服務於資安構面是否有風險 □分析程式內部登入於資安構面是否有風險 □於「威脅建模」(Threat Modeling)逐一列出

				□其他：
2.4.2	開發實作階段（Implementation） 應避免常見弱點及發展控制措施	◎	□適用 □不適用 說明：	□透過 HTTPS 傳輸加密 □對稱或非對稱式加密資料庫 □其他：
2.4.3	驗證測試階段（Verification）	◎	□適用 □不適用 說明：	□源碼檢測(靜態分析) □弱點掃描(動態分析) □滲透測試(動態分析) □其他：
2.4.4	部署維運階段（Deployment & Maintenance） 透過版本控制工具，掌握版本是否為最新版，並隨時更新版本、修補漏洞，以維持版本的最佳化	◎	□適用 □不適用 說明：	□更新版本 □修補漏洞 □其他：
2.5 資料安全管理				
2.5.1	資料傳輸	◎	□適用 □不適用 說明：	□IT 系統遠端存取連線軟體升級至企業版本 □SQL（結構化查詢語言）更新至最新版 □個資透過 API 傳輸時做有效加密、隱碼遮罩 □要求個資提供方透過 API 傳輸時，做有效加密及隱碼遮罩 □其他：
2.5.2	資料庫防護	◎	□適用 □不適用 說明：	□系統內採用加解密機制存取設定資料 □資料庫、資料表內個資採用加解密機制存取資料 □增設存取 log 紀錄 □其他：
2.6 系統存取控制				
2.6.1	加強帳號註冊或註銷等權限管理		□適用 □不適用 說明：	□帳號最低權限原則 □不共用帳號 □其他：
2.6.2	於系統中布建使用者身分		□適用	□於系統中布建使用者

	配置程序		□不適用 說明：	身分配置程序
2.6.3	管理使用者密碼資訊及特權存取權限應被限制與管理		□適用 □不適用 說明：	□限制與管理使用者存取權限
2.6.4	定期檢視使用者權限		□適用 □不適用 說明：	□半年至少 1 次檢視使用者權限 □1 年至少____次檢視使用者權限
2.6.5	客戶登入後台之管控	◎	□適用 □不適用 說明：	□協助客戶強化登入後台資料庫密碼複雜度 □協助客戶強化登入後台資料庫採取多因子認證 □限縮客戶有權限進入後台系統（包含下載權限）之人數 □縮短客戶帳號的登入閒置時間，並於閒置過久時強制登出 □其他：
2.7 系統維護				
2.7.1	不於非上班時間處理客戶突發問題 以確保所有系統操作皆由公司 IP 進行	◎	□適用 □不適用 說明：	□採取_____措施使員工皆由公司 IP 進行系統操作
2.7.2	第三方資安健檢	◎	□適用 □不適用 說明：	□定期由第三方資安廠商執行資安健檢 □佈署端點防護軟體 □其他：
2.7.3	發現的資訊服務系統或網站平台的弱點列表及控制措施	◎	□適用 □不適用 說明：	□自主及尋求第三方協助發現的資訊服務系統或網站平台的弱點列表及控制措施 □提出預防或避免攻擊之作法供線上驗證 □其他：
2.8 人員資安認知				

2.8.1	人員資安職能訓練		□適用 □不適用 說明：	□規劃訓練藍圖 □辦理訓練頻率：
2.8.2	定期電子郵件社交工程演練		□適用 □不適用 說明：	□演練頻率：每半年至少1次 □演練內容：
3.法遵面				
3.1 法規要求事項之識別				
3.1.1	個人資料保護法及個人資料保護法施行細則		□適用 個人資料保護法及個人資料保護法施行細則	□個人資料保護法 □個人資料保護法施行細則
3.1.2	製造業及技術服務業個人資料檔案安全維護計畫管理辦法		□適用 個人資料保護法	□製造業及技術服務業個人資料檔案安全維護管理辦法
3.1.3	委託者主管機關之相關法令規範 例如：經濟部商業司法令、衛生福利部法令、教育部法令	◎	□適用 □不適用 說明：	□《網際網路零售業及網際網路零售服務平台業個人資料檔案安全維護計畫及業務終止後個人資料處理作業辦法》 □《觀光旅館業個人資料檔案安全維護計畫辦法》 □《私立兒童課後照顧服務中心個人資料檔案安全維護計畫實施辦法》 □《短期補習班個人資料檔案安全維護計畫實施辦法》 □其他：
3.2 契約要求事項之識別				
3.2.1	定義所提供 ERP 服務的安全使用環境 於資訊安全文件中敘明資訊服務系統的安全使用環境，應配合採行哪些資訊安全配套措施或工具，以及資料透過 API 傳輸及存取過程之資安防護策略	◎	□適用 □不適用 說明：	□資訊安全文件中敘明資訊服務系統安全使用環境 □資訊安全配套措施： □資訊安全配套工具： □資料傳輸及存取過程之資安防護策略： □其他：

3.2.2	系統商之委託客戶義務	◎	□適用 □不適用 說明：	□一年___次更新各式系統及軟體版本 □配合加裝指定之資訊安全配套措施或工具 □客戶自建伺服器者之連接加密等級 □客戶之電腦設備不可安裝非法軟體 □避免多人共用後臺登入之帳密 □離開電腦或下班時應從後臺登出 □一周___次針對登入後臺電腦使用掃毒 □一年___次社交工程演練 □其他：
3.2.3	系統商端義務	◎	□適用 □不適用 說明：	□確保網頁安全（SSL 加密） □設計具加密功能的通道使客戶傳輸機敏資料 □設計傳輸機敏資料時隱碼（遮罩）不必要資訊 □管控客戶存取權限 □一年___次做社交工程演練 □其他：
3.2.4	租用雲端主機時釐清責任	◎	□適用 □不適用 說明：	□釐清連接架構 □確認資料存放和保護管理責任分配 □其他：
4.作業流程面				
4.1 控制措施				
4.1.1	控制措施 資訊安全政策、資訊安全組織、人力資源安全、資產管理、存取控制、密碼學、實體及環境安全、操作安全、通訊安全、系統		□適用 □不適用 說明：	□逐步承諾內容： □全部承諾

	獲取開發及維護、供應者關係、資訊安全事故管理、資訊安全持續、遵循性等 14 個項目			
4.2 資訊安全管理的四階文件				
4.2.1	第一階文件：安全手冊 最高指導文件		□適用 □不適用 說明：	□資訊安全政策 □ISO27001 適用性聲明 □其他國際標準之適用性聲明
4.2.2	第二階文件：管理辦法 企業資訊安全管理制度文件化		□適用 □不適用 說明：	□ □
4.2.3	第三階文件：作業程序 規定標準作業細節		□適用 □不適用 說明：	□ □
4.2.4	第四階文件：紀錄表單 作業流程實際作業		□適用 □不適用 說明：	□ □
5.持續與改善				
5.1.1	導入日誌分析系統與事件反應機制 用以作為存錄與監控，以識別、蒐集、獲取及保存可作為證據之資訊		□適用 □不適用 說明：	□導入日誌分析系統 □導入事件反應機制 □其他：
5.1.2	使用紀錄及軌跡資料證據保存		□適用 □不適用 說明：	□紀錄資料使用紀錄 □紀錄自動化機器設備之軌跡資料 □落實執行資訊安全管理措施之證據 □其他：
5.2.1	內部資安稽核機制 一年至少一次		□適用 □不適用 說明：	□1 年至少____次內部資安稽核 □提出評估報告 □採行改善機制： □其他：
5.2.2	第三方資安稽核驗證或檢測		□適用 □不適用 說明：	□委請第三方資安稽核 □委請第三方驗證機構進行資安稽核

				□委託資安公司進行資安健檢並提出檢測報告 □其他
5.3.1	持續改善措施		□適用 □不適用 說明：	□以 PDCA 之政策說明進行資訊安全政策之持續與改善 □討論會議製作書面紀錄以為佐證 □其他：

資料來源：本指引自製

附錄三、配合主管機關調查之佐證資料範例

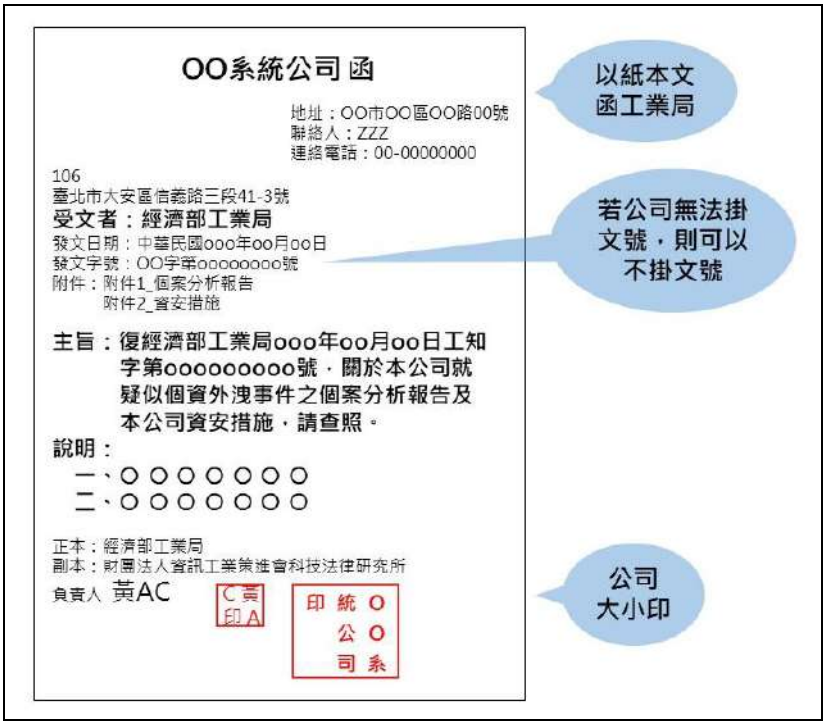

圖 13 函復主管機關封面範例
資料來源：本指引自製

（一）個案分析報告

1. 與委託客戶間之關係：

(1) 系統架構圖及系統架構文字說明

範例：本公司提供本次個資事故涉及之系統的系統架構圖，包含系統的網路架構圖、個資傳輸及存放地點架構圖等如下：

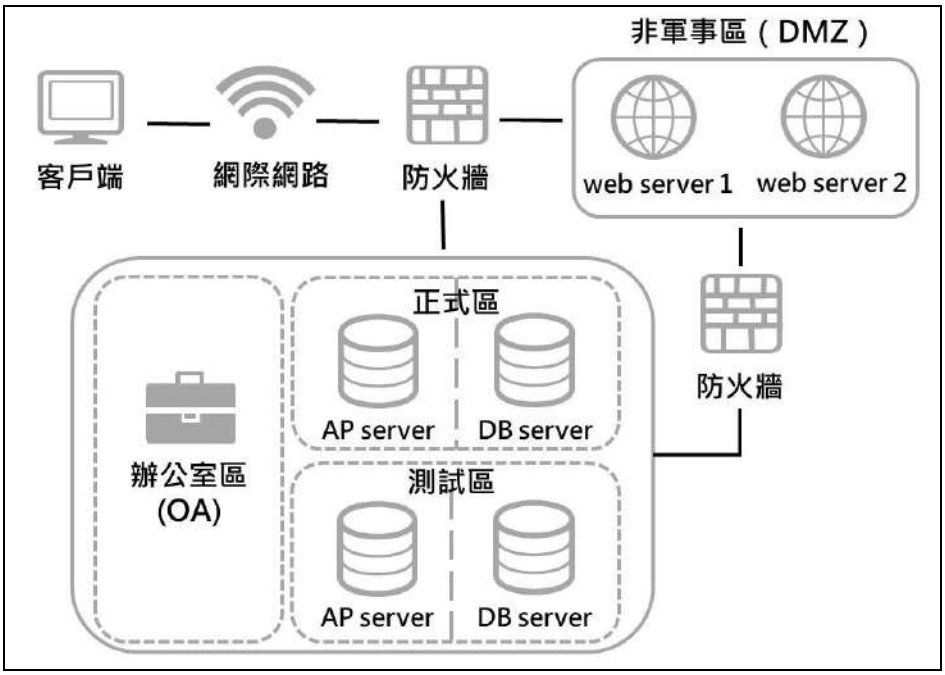

圖 14 系統網路架構圖範例
資料來源：本指引自製

圖 10 為系統網路架構圖範例。圖 11 為個資傳輸及存放地點的架構圖，從圖中能得知，本公司之系統與客戶間之資料交換方式為○○○○○（例如：以 API 方式介接時如何認證、憑證密碼如何存放等）。

客戶消費者下單至出貨過程中，消費者個資傳輸過程及其傳輸過程中個資可能存放的地點有○○○○○、○○○○○、○○○○○等（例如電商客戶端、系統商公司處、雲端主機處等）。

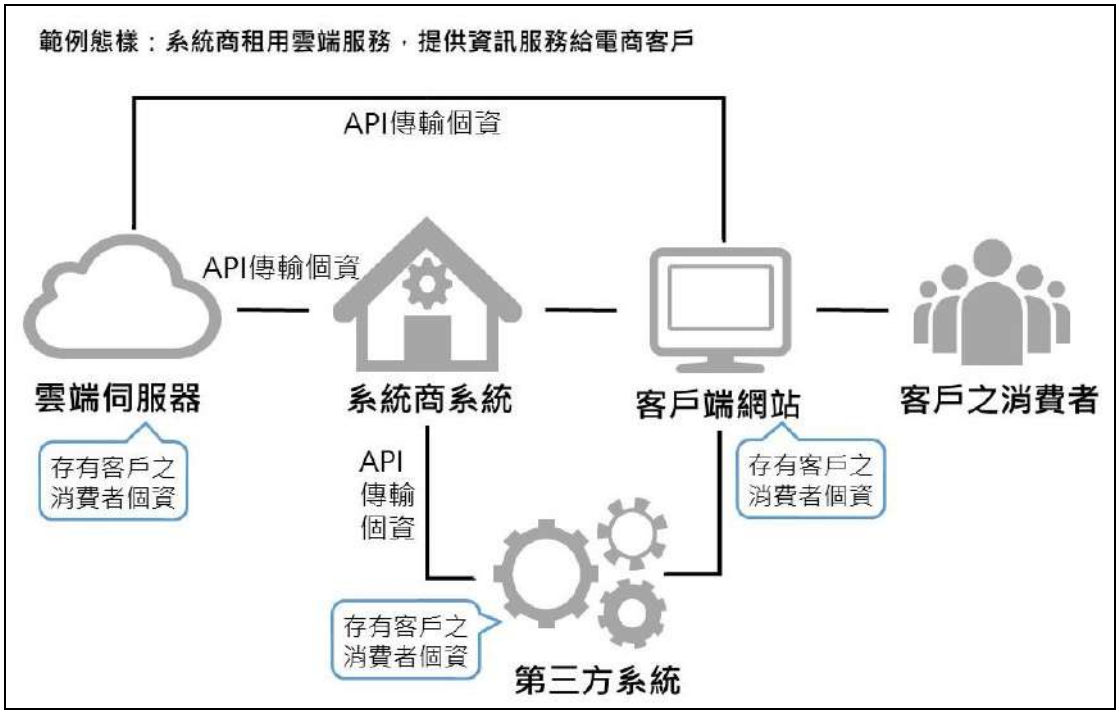

圖 15 個資傳輸及存放地點架構圖範例
資料來源：本指引自製

(2) 公司對客戶之資安環境要求及相關權限控管

範例：本公司對客戶之相關資安環境要求，包含○○○○○（舉例：必須安裝防毒軟體、雙重驗證（2FA）登入、白名單才能允許串接、登入及存取權限控管方式等。）

(3) 公司與客戶間之契約要求內容

範例：本公司對客戶之契約要求，包含○○○○○（舉例：雙方資料存取權限、雙方資料存放管理責任、雙方應盡個資安全維護義務、客戶資安環境要求、貴公司資安防禦措施等權責約定內容。）

2. 個資外洩發生的可能原因

範例：本公司於○○○年○○月○○日○○：○○知悉發生個資外洩事件，初步調查後發現，○○○年○○月○○日○○：○○時，有不明駭客利用○○○發動攻擊，在系統○○○處植入○○程式，竊取消費者資料，導致個資外洩。截至○○○年○○月至○○月止，已掌握○○○筆詐騙通報案，包含「○○」等○○間客戶網站的消費者受影響。

3. 事件發生前所採行之平時資料維護措施

(1) 資料傳輸安全之維護措施

範例：a.本公司透過 API 傳輸個資時，將個資作有效之加密或隱碼遮罩，以防不幸發生個資外洩時，減少可被識別的資訊；b.本公司透過 API 接受客戶之委託第三方所傳輸之個資時，有要求該些提供個資者將個資最小化，並作有效之加密或隱碼遮罩後再進行傳輸。

(2) 資料庫保管說明

範例：a.資料庫有加密，加密方式為◯◯◯；b.資料庫的存取管控方式為◯◯◯；c.資料庫有存取 log 紀錄；d.資料庫密鑰與資訊系統資料的存放位置有區隔，區隔方式為◯◯◯。

(3) 資安風險自評

範例：檢附 1 年內及事件發生時[20]透過網頁滲透測試（Penetration Test）、系統或網頁弱點掃描（Vulnerability Scanning）、網頁原始碼掃描（源碼檢測，Code Review）等完整的資安檢測報告如下。[21]

另外，由於本公司發現檢測報告中出現中、高風險，嗣後將主動補充沒有中、高風險結果的複測檢測報告，以作為有進行改善的佐證。

---

[20] 事件發生時若來不及進行掃描，宜附上預備進行資安檢測的證明，例如外部資安公司的檢測服務購買證明。

[21] 建議系統商可先於工業局委託工研院所建置的「SECPAAS 資安整合服務平台」網站（https://secpaas.org.tw/），尋找試用服務（https://secpaas.org.tw/services/）或各種產品服務的廠商資訊（https://secpaas.org.tw/product/）（最後瀏覽日：2021/12/20）。

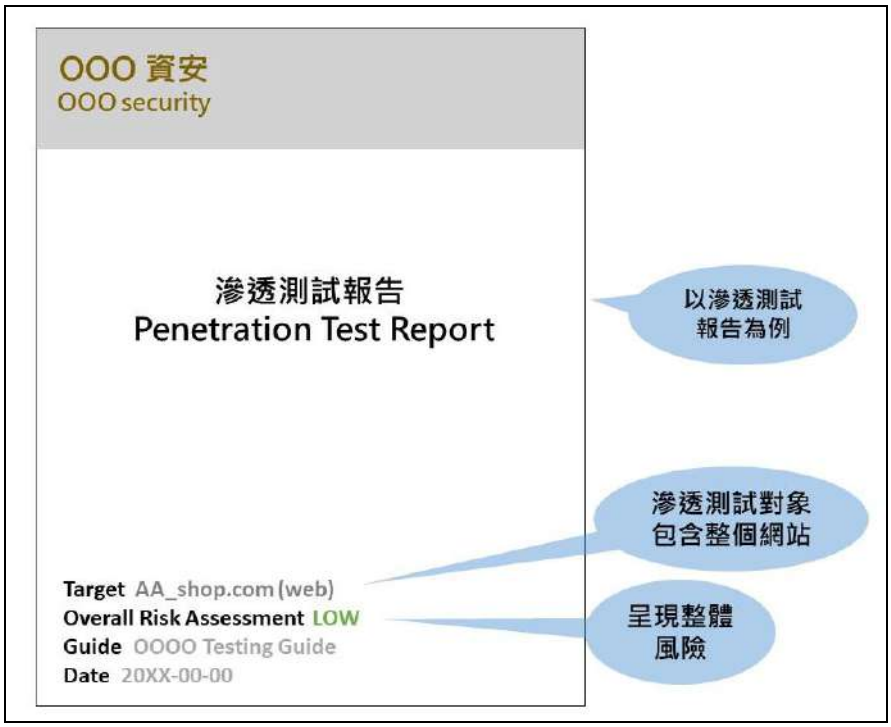

圖 16 滲透測試報告封面截圖範例[22]

資料來源：本指引自製

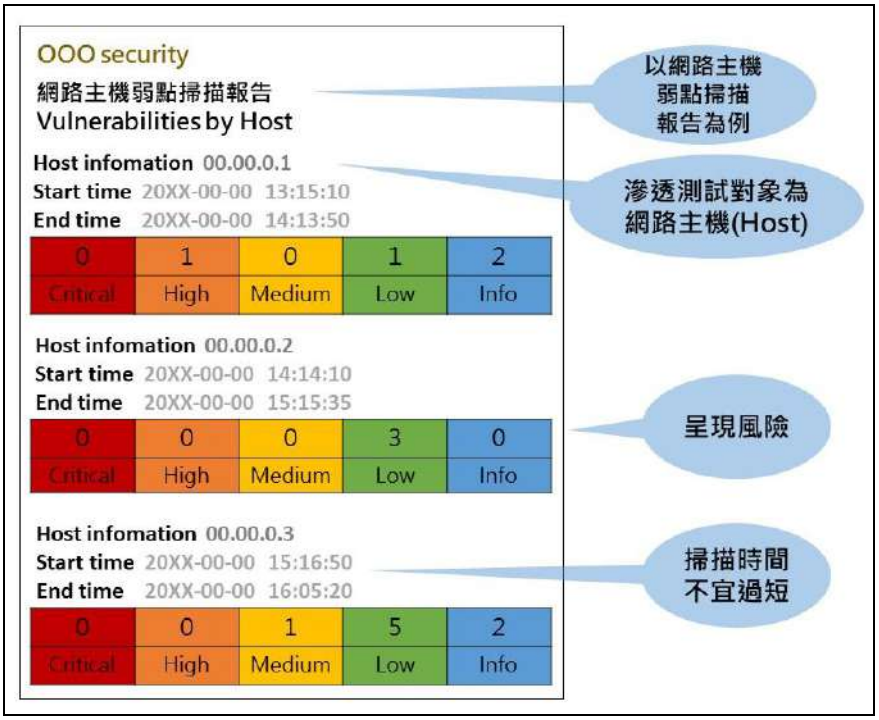

圖 17 弱點掃描報告封面截圖範例

資料來源：本指引自製

[22] 本指引僅提供封面截圖範例，系統商實際提供各種資安風險自評的檢測報告時，應提供檢測工具所呈現的原始完整報告。

4. 事件發生時所採取之應變措施

(1) 有以適當方式及內容通知各客戶之佐證資料

範例：

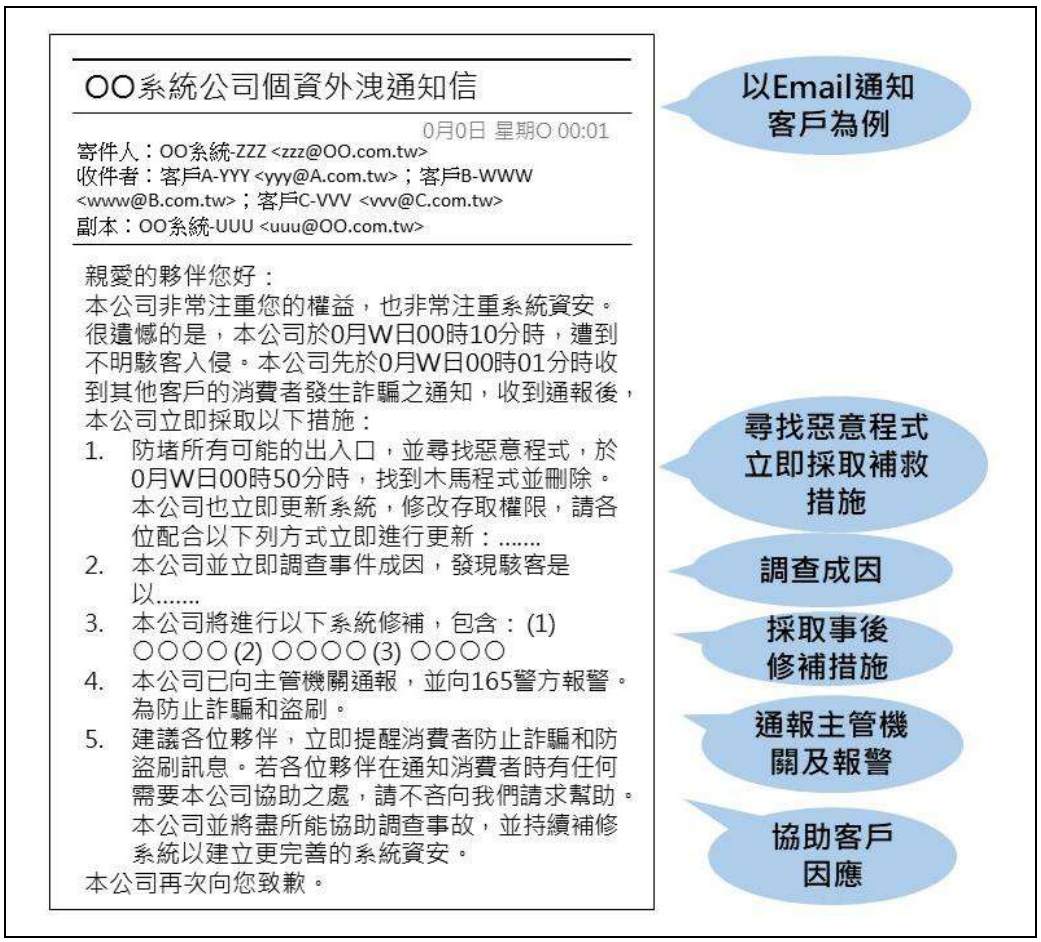

圖 18 Email 通知客戶截圖範例

資料來源：本指引自製

(2)　有協助客戶通知消費者之佐證資料

範例[23]：

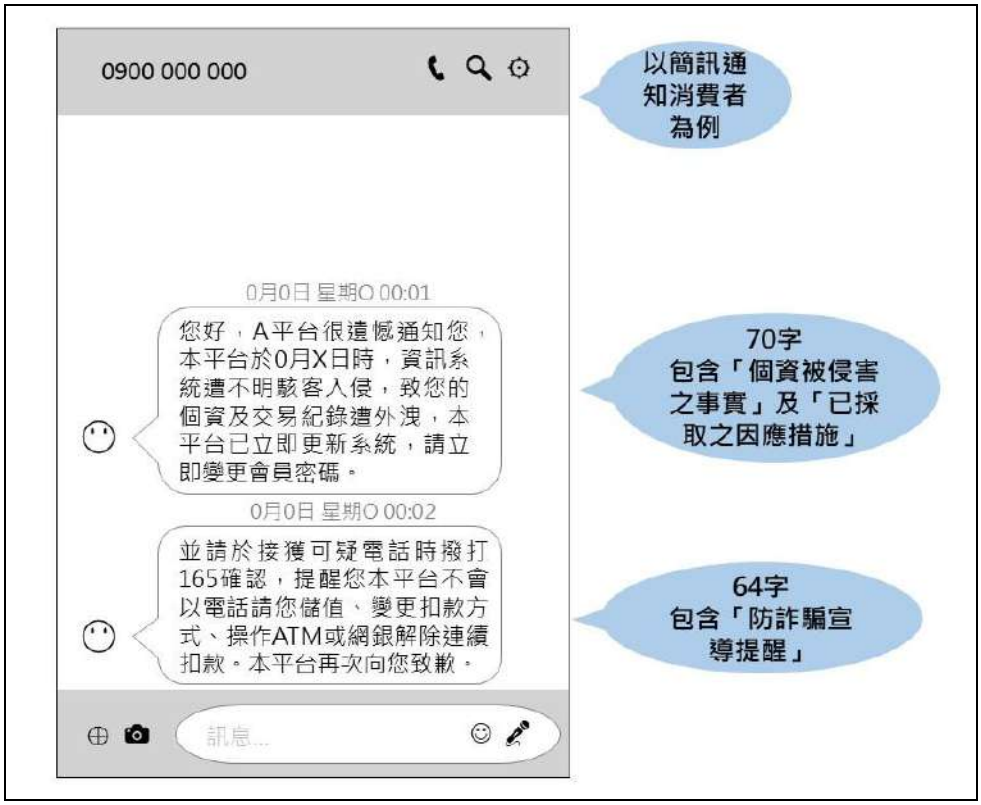

圖 19 簡訊通知消費者截圖範例
資料來源：本指引自製

(3)　刪除惡意程式之佐證資料

範例：○○○年○○月○○日○○：○○時，已透過惡意程式偵測軟體發現系統○○○處被植入木馬程式，已立即刪除。

(4)　調查事件成因之佐證資料

範例：個資外洩時，防火牆、DB 等的 log 紀錄及○○○年○○月○○日○○：○○時，透過調取防火牆及資料庫 log 發現，有不明境外 IP 以○○○方式進入資料庫。疑似係因處存有漏洞，分析報告如下：○○○○○○。

[23] 亦可參考經濟部商業司，〈非公務機關發生個資事故時對個資當事人通知之範例〉，https://gcis.nat.gov.tw/mainNew/matterAction.do?method=showFile&fileNo=t70466_p （最後瀏覽日：2021/12/20）。

5. 事件發生後所採行之改善措施

範例：本公司於事件發生後，持續採取以下改善措施。(1)建置即時監測告警系統；(2)限縮客戶機構的系統使用權限；(3) 逐步進行機敏性資料庫欄位加密；(4)委請○○資安公司強化現有基礎架構，並針對調查發現的漏洞，採取以下措施：○○○○○○。

（二）公司資安保護措施

1. 資料安全管理

範例：本公司有採取加密措施、對於備份資料之保護措施、保存與傳輸安全之維護措施等；採取之資訊系統之安全維護措施，包括：防火牆或其他入侵偵測設備、防毒措施、系統與程式漏洞檢視與修補、使用者認證機制、異常存取資料行為之監控機制、系統測試之個資保護機制等。詳述如下：○○○○○○。(請詳見本文第四章、一、(六)、1；第四章、二、(二)、5)

2. 人員安全管理

範例：本公司有進行人員保密措施、存取權限之控制、人員離退時之資料返還等。詳述如下：○○○○○○。(請詳見本文第四章、一、(六)、2)

3. 設備安全管理

範例：本公司對存有個人資料之紙本、磁碟、磁帶、光碟片、微縮片、積體電路晶片、電腦、自動化機器設備及其他媒介物（以下簡稱儲存媒介物），所採取之設備安全管理措施，包括對存放儲存媒介物之環境，所取之適當的之進出管制措施等。詳述如下：○○○○○○。(請詳見本文第四章、一、(八))

4. 認知宣導及教育訓練

範例：本公司 1 年舉辦○次個資及資安教育訓練及宣導活動；半年實施○次社交工程演練。以下為教育訓練紀錄截圖及社交工程演練紀錄截圖。

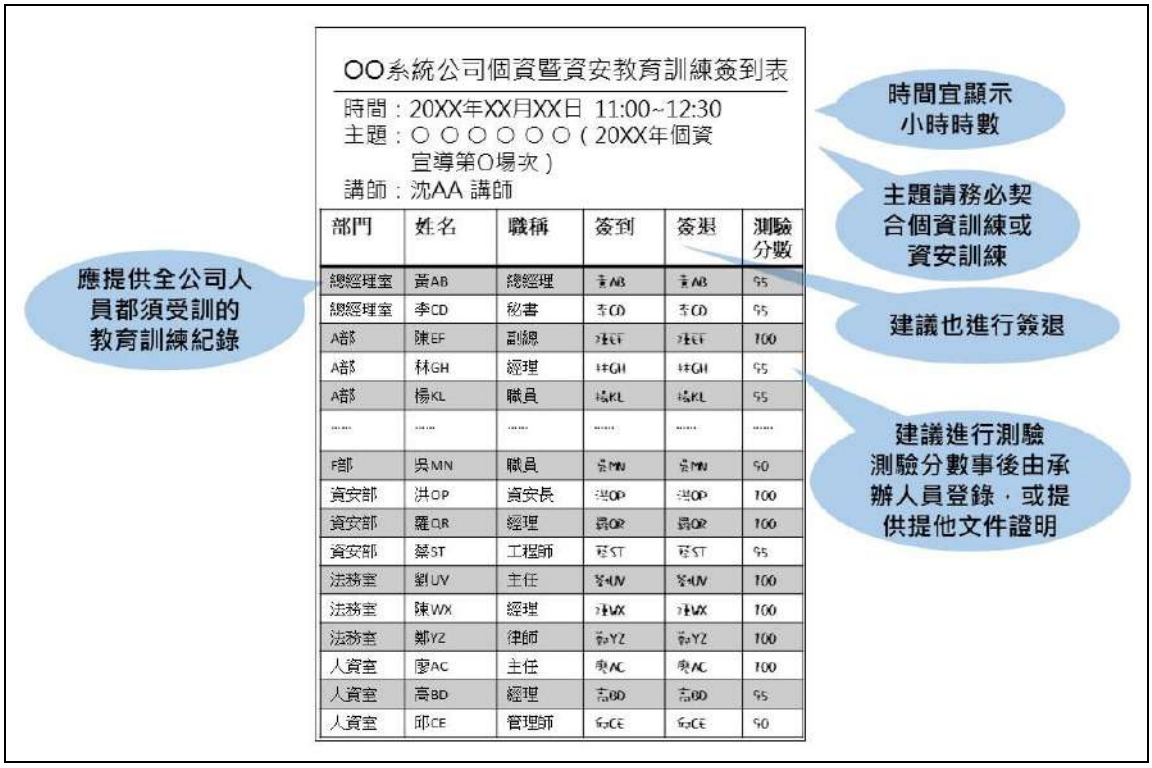

圖 20 教育訓練簽到表截圖範例

資料來源：本指引自製

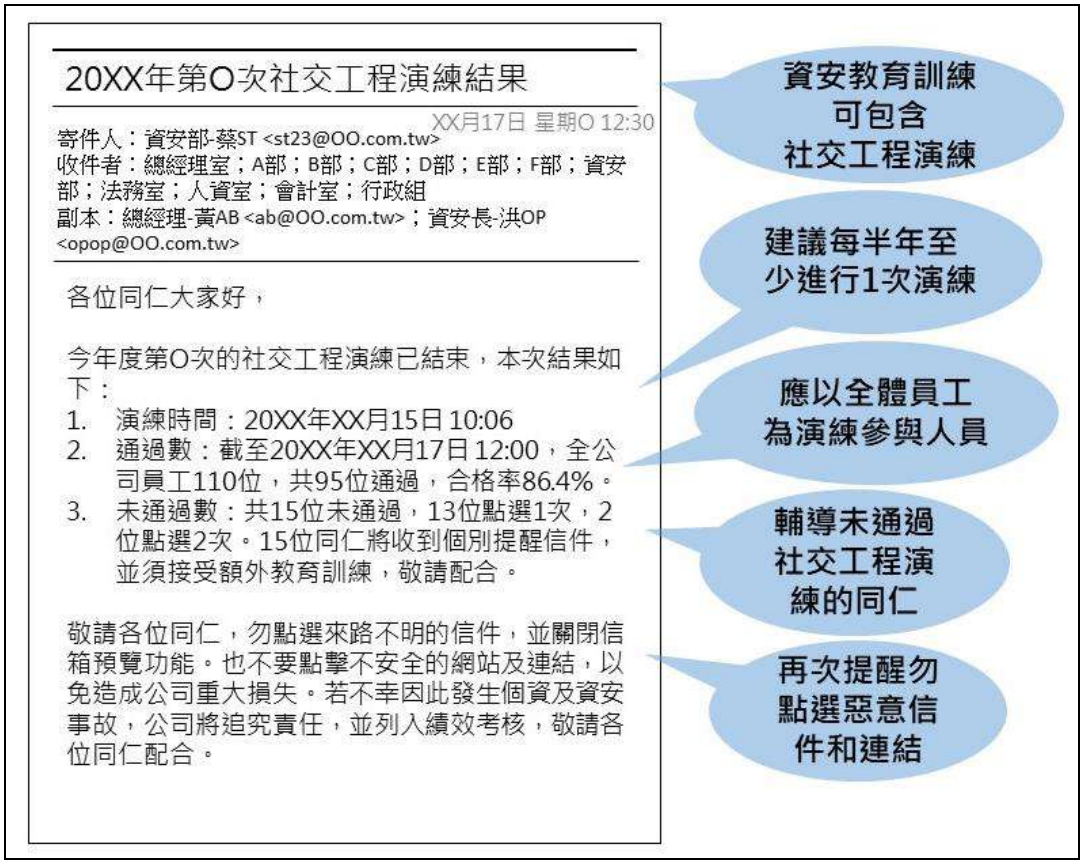

圖 21 社交工程演練截圖範例

資料來源：本指引自製

資訊服務業者
落實個人資料保護暨資訊安全 參考指引

編撰 中華民國110年12月